

John Petriello (JJP-6545)  
LEVY, EHRLICH & PETRIELLO  
60 Park Place  
Newark, New Jersey 07102  
Telephone: (973) 854-6700  
Facsimile: (973) 596-1781

Attorneys for Plaintiffs  
ECHOSTAR SATELLITE L.L.C.,  
ECHOSTAR TECHNOLOGIES L.L.C.  
and NAGRASTAR LLC

**FILED**  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.  
★ AUG 13 2010 ★

UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF NEW YORK

BROOKLYN OFFICE

DISH NETWORK L.L.C., a Colorado  
Limited Liability Company, ECHOSTAR  
TECHNOLOGIES L.L.C., a Texas Limited  
Liability Company, and NAGRASTAR LLC,  
a Colorado Limited Liability Company,

Plaintiffs,

v.

MUNID RAMKISSOON, an individual,  
OOTRA RAMKISSOON, an individual, and  
DOES 1-10,

Defendants.

Case No.

**MISC 10 - 0546**

D.N.J. Case No. 2:09-CV-01143-DEP

**MAUSKOPF, J.**

**DECLARATION OF CHAD M. HAGAN IN  
SUPPORT OF DISH NETWORK'S  
MOTION TO COMPEL THIRD-PARTY  
CABLEVISION SYSTEMS CORP. TO  
PRODUCE DOCUMENTS IN RESPONSE  
TO SUBPOENA**

I, Chad M. Hagan, declare:

1. I am a principal of the law firm of Hagan Noll & Boyle LLC and am duly licensed to practice law in the states of Texas and Colorado. I have also been admitted *pro hac vice* for purposes of the *DISH Network L.L.C. et al. v. Munid Ramkissoon et al.* litigation pending in the District of New Jersey, and I am authorized to make this declaration in that capacity. I make this declaration of my own personal knowledge and, if called upon to testify, could and would testify competently as stated herein.

2. Attached as **Exhibit 1** is a true and correct copy of Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C., and NagraStar LLC's (collectively "Plaintiffs") Complaint filed against Munid Ramkissoon, Ootra Ramkissoon and Does 1-10 (collectively "Defendants") on or about December 4, 2009.

3. Attached as **Exhibit 2** is a true and correct copy of Plaintiffs' Amended Statement of Claim filed against Ravindranauth Ramkissoon, among other individuals and entities, on or about July 6, 2009.

4. After serving Defendants with a copy of Plaintiffs' Complaint, Plaintiffs requested that Defendants produce their DISH Network equipment and computers for inspection. Defendants initially agreed to produce the devices, but then claimed they were stolen out of their vehicle during transport to their attorneys' office. Attached as **Exhibit 3** is a true and correct copy of an email exchange between Plaintiffs' counsel and Defendants' counsel regarding the alleged "theft".

5. Attached hereto as **Exhibit 4** is a true and correct copy of Defendants' Response to Plaintiffs' Interrogatories.


6. On July 14, 2010, counsel for the parties participated in a status conference before the District of New Jersey Court. During the conference, Defendants' counsel admitted that Defendants have maintained their cable television service in addition to their DISH Network satellite television account.

7. On or about July 15, 2010, Plaintiffs issued a subpoena to Cablevision Systems Corp. d/b/a Optimum ("Cablevision") pursuant to Rule 45 of the Federal Rules of Civil Procedure. Attached as **Exhibit 5** is a true and correct copy of the subpoena to Cablevision.

8. On or about July 20, 2010, Cablevision responded to Plaintiffs' subpoena by letter stating that they are withholding the production of responsive documents pursuant to section 551(c)(2)(B) of the Cable Communications Privacy Act of 1984 until they receive a court order mandating such disclosure. Attached as **Exhibit 6** is a true and correct copy of Cablevision's response to Plaintiffs' subpoena.

9. Attached as Exhibit 7 is a true and correct copy of the Order of the Ontario Superior Court of Justice dated February 23, 2010 in the matter of *DISH Network L.L.C. et al. v. Ravindranauth Ramkissoo et al.*

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 9, 2010 in Houston, Texas.

  
Chad M. Hagan

Chad M. Hagan (*pro hac vice* pending)  
David M. Noll (*pro hac vice* to be filed)  
Joseph H. Boyle (*pro hac vice* to be filed)  
HAGAN NOLL & BOYLE LLC  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, Texas 77024  
Telephone: (713) 343-0478  
Facsimile: (713) 758-0146

John Petriello (JJP-6545)  
LEVY, EHRLICH & PETRIELLO  
60 Park Place  
Newark, New Jersey 07102  
Telephone: (973) 854-6700  
Facsimile: (973) 596-1781

Attorneys for Plaintiffs  
ECHOSTAR SATELLITE L.L.C.,  
ECHOSTAR TECHNOLOGIES L.L.C.  
and NAGRASTAR LLC

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

DISH NETWORK L.L.C., a Colorado  
Limited Liability Company, ECHOSTAR  
TECHNOLOGIES L.L.C., a Texas Limited  
Liability Company, and NAGRASTAR LLC,  
a Colorado Limited Liability Company,

Plaintiffs,

v.

MUNID RAMKISSOON, an individual,  
OOTRA RAMKISSOON, an individual, and  
DOES 1-10,

Defendants.

Civil Action No.

**PLAINTIFFS' ORIGINAL COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs DISH Network L.L.C., a Colorado limited liability company with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112, EchoStar Technologies L.L.C., a Texas limited liability company with its principal place of business

located at 90 Inverness Circle East, Englewood, Colorado 80112, and NagraStar LLC, a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112, bring this action against Defendants Munid and Ootra Ramkissoon, individuals who, upon information and belief, reside at 5 Seasons Glen Dr., Morris Plains, New Jersey, 07950, and Does 1-10, whose identities and residences are presently unknown to Plaintiffs. Plaintiffs allege as follows:

### **INTRODUCTION**

1. Plaintiffs bring this action against Defendants Munid and Ootra Ramkissoon and Does 1-10 ("Defendants") for unlawfully using DISH Network satellite receivers and access cards to obtain decryption keys or control words for unscrambling encrypted DISH Network satellite television programming, and for distributing those keys or control words over the internet in order to allow others to view DISH Network satellite television programming without authorization from or payment to Plaintiffs.

2. Defendants' actions violate the Communications Act, 47 U.S.C. § 605, the Digital Millennium Copyright Act, 17 U.S.C. § 1201, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, and state law.

3. Plaintiffs bring this action to restrain these illegal activities and for other relief described in this Complaint.

### **PARTIES**

4. Plaintiff DISH Network L.L.C. is a Colorado limited liability company with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112, Arapahoe County. Plaintiff DISH Network L.L.C.'s sole member is DISH DBS Corporation, a Colorado Corporation, which in turn is an indirect wholly owned subsidiary of DISH Network

Corporation, a Nevada Corporation. DISH Network Corporation is publicly owned and traded on the NASDAQ national market under the symbol "DISH."

5. Plaintiff EchoStar Technologies L.L.C. is a Texas limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112, Arapahoe County. Plaintiff EchoStar Technologies L.L.C.'s sole member is EchoStar Corporation, a Nevada Corporation. EchoStar Corporation is publicly owned and traded on the NASDAQ national market under the symbol "SATS." EchoStar is the designer and manufacturer of DISH Network satellite receivers described herein.

6. Plaintiff NagraStar LLC is a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112, Arapahoe County. NagraStar is a joint venture between EchoStar Corporation and the Kudelski Group, a group of companies headquartered in Switzerland. Plaintiff NagraStar L.L.C.'s sole members are EchoStar Corporation and Kudelski SA. EchoStar Corporation is identified in paragraph 5 above. Kudelski SA has its principal place of business at 22-24, Route de Genève, 1033 Cheseaux, Switzerland and is listed on the SIX Swiss Exchange under the symbol "KUD." NagraStar provides the technical measures that control access to DISH Network's copyrighted works described herein.

7. Upon information and belief, Defendants Munid and Ootra Ramkissoon are residents of Morris Plains, New Jersey.

8. Upon information and belief, Does 1-10 are persons, the identity of whom is presently unknown to Plaintiffs but known to Defendants Munid and Ootra Ramkissoon, who operated, assisted with, or participated in establishing or operating internet control word sharing servers, also known as internet key sharing or "IKS" servers, including but not limited to using access cards and receivers provided by Defendants Munid and Ootra Ramkissoon to operate or

support an IKS server, thereby facilitating the unauthorized reception of DISH Network programming without authorization from or payment to Plaintiffs.

### **JURISDICTION AND VENUE**

9. This action arises under the federal Communications Act, 47 U.S.C. § 605, the Digital Millennium Copyright Act, 17 U.S.C. § 1201, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, and state law.

10. This Court has original jurisdiction pursuant to 28 U.S.C. § 1331, 47 U.S.C. § 605(e)(3)(A), 17 U.S.C. § 1201(a), and 18 U.S.C. 2520(a), and has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) over the state law claims asserted herein.

11. Personal jurisdiction and venue are proper in this District pursuant to 28 U.S.C. § 1391(b), because a substantial portion of the events or omissions giving rise to the claims herein occurred in this District and because Defendants Munid and Ootra Ramkissoo reside in this District.

### **FACTUAL BACKGROUND**

12. DISH Network is a satellite television company, delivering hundreds of channels movies, sports, and general entertainment services to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price).

13. DISH Network contracts and pays for the distribution rights of copyrighted programming from networks, affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers, including HBO, SHOWTIME, ESPN, Cinemax, and Disney.

14. Because DISH Network generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain

distribution rights for programming is dependent upon preventing unauthorized reception of DISH Network Programming, DISH Network's video channels, except for certain promotional channels, are all digitally secured and encrypted.

15. DISH Network digitally compresses and digitizes its satellite television programming and then encrypts (electronically scrambles) it before transmitting it to its customers in order to prevent unauthorized viewing of the programming by non-subscribers. DISH Network transmits its encrypted satellite signal to satellites above the earth, which in turn transmit the encrypted programming back down to customers who are equipped with DISH Network receiving equipment consisting of a small satellite dish and a DISH Network integrated receiver/decoder, also called a satellite receiver.

16. DISH Network's encrypted satellite signal is received by a customer's satellite dish and relayed by a cable wire to the consumer's DISH Network satellite receiver. Inside each DISH Network satellite receiver is a removable credit-card sized access card that contains a microprocessor. On some newer models of satellite receiver, the access card is integrated directly into the satellite receiver itself and is not removable. This access card works with the receiver to decrypt or descramble the encrypted DISH Network satellite signal.

17. Each DISH Network satellite receiver and each access card are assigned unique serial numbers and those numbers are used by DISH Network when activating the satellite receiving equipment and to ensure that the equipment decrypts the DISH Network programming that the customer is authorized to receive as part of their subscription package and pay-per-view purchases.

18. When a DISH Network satellite receiver receives encrypted DISH Network satellite signals it locates a special part of the satellite transmission known as the encrypted entitlement control message and sends that encrypted entitlement control message to the access

card in the satellite receiver. The access card checks to see what channels the customer is authorized to view as part of their subscription and provides the secret control word for those channels back to the satellite receiver. The satellite receiver uses the control word to descramble only those channels that the subscriber is authorized to see as part of their subscription package.

**DEFENDANTS' WRONGFUL CONDUCT<sup>1</sup>**

19. Beginning at a time unknown and continuing to the present, Defendants have engaged in illegal and improper acts for the purposes of obtaining DISH Network satellite television programming and the encrypted control words that protect access to the copyrighted satellite television programming and distributing those control words over the internet.

20. Upon information and belief, Defendants or others working in conjunction with Defendants operate an IKS server.

21. This IKS server has multiple DISH Network satellite receivers and/or access cards attached to it that are used to decrypt DISH Network satellite television programming and obtain the control words for decrypting that programming. The server gathers these now-unencrypted control words and sends them over the internet to end-users who use the control words to decrypt DISH Network satellite television programming without paying a subscription fee.

22. There are numerous black and gray market satellite receivers imported from Korea that are designed and programmed to use these stolen and decrypted control words to intercept and decrypt DISH Network satellite television programming by interacting with an IKS server.

---

<sup>1</sup> Plaintiffs' allegations related to Defendants' wrongful conduct are based upon the investigation Plaintiffs have completed to date, upon information and belief, and with the reasonable belief that further investigation and discovery in this action will lead to additional factual support.

23. On or about July 19, 2009, Defendants Munid and Ootra Ramkissoo created a residential account for DISH Network satellite television service, using a purported residential service address at 5 Seasons Glen Dr., Morris Plains, New Jersey 07950. Defendants Munid and Ootra Ramkissoo activated three DISH Network satellite receivers and access cards associated with the account. Plaintiffs' investigation confirmed that at least one of the satellite receivers and access cards activated by Defendants Munid and Ootra Ramkissoo is being used to supply Plaintiffs' control words to others in violation of federal and state law and the customer agreement.

24. Upon information and belief, Defendants Munid and Ootra Ramkissoo created this residential account for the purpose of obtaining DISH Network television programming and control words and distributing those control words over an IKS server operated by Defendants and/or those acting in conjunction with Defendants.

25. At the time Defendants Munid and Ootra Ramkissoo created this residential account, Defendants misrepresented to DISH Network that the intended purpose and use of DISH Network programming was private viewing. That is, Defendants Munid and Ootra Ramkissoo contracted for residential television service when in truth and fact Defendants knew and intended to use DISH Network programming and access cards to supply the control words for television content to others over the internet and without Plaintiffs' authorization or consent and in violation of federal and state law, including DISH Network's rights under the customer agreement.

26. At the time Defendants Munid and Ootra Ramkissoo created the residential account, Defendants misrepresented to DISH Network the intended location where DISH Network programming would be viewed. That is, Defendants Munid and Ootra Ramkissoo supplied a purported residential service address when in truth and fact Defendants knew and

intended that DISH Network programming would be viewed at multiple other locations that obtained the control words from the IKS server.

27. Defendants' wrongful conduct has caused and continues to cause significant and irreparable harm to Plaintiffs by depriving Plaintiffs of subscriber and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, and interfering with Plaintiffs' prospective business relations.

**COUNT 1**

**RECEIVING AND ASSISTING OTHERS IN RECEIVING  
SATELLITE SIGNALS IN VIOLATION OF 47 U.S.C. § 605(a)**

28. Plaintiffs repeat and reallege the allegations in all preceding paragraphs as if fully set forth herein.

29. By distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, Defendants have received and assisted others in receiving Plaintiffs' encrypted satellite transmissions of television programming and control words without authorization by Plaintiffs, in violation of 47 U.S.C. § 605(a).

30. Defendants' violations have injured Plaintiffs, including, by way of example, depriving Plaintiffs of subscription revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, and interfering with Plaintiffs' prospective business relations.

31. Defendants have violated 47 U.S.C. § 605(a) willfully and for purposes of direct or indirect commercial advantage or private financial gain.

32. Defendants knew or should have known that receiving or assisting other persons in receiving Plaintiffs' encrypted satellite transmissions of television programming and control

words without authorization by or proper payment to Plaintiffs was and is illegal and prohibited. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendants will continue to violate 47 U.S.C. § 605(a).

**COUNT 2**

**INTERCEPTING AND PROCURING OTHERS TO INTERCEPT  
SATELLITE SIGNALS IN VIOLATION OF 18 U.S.C. § 2511(1)(a)**

33. Plaintiffs repeat and reallege the allegations in all preceding paragraphs as if set forth fully herein.

34. By distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, Defendants have intercepted, endeavored to intercept and/or procured others to intercept or endeavor to intercept Plaintiffs' encrypted satellite transmissions of television programming and control words, without authorization by Plaintiffs, in violation of 18 U.S.C. § 2511(1)(a).

35. Plaintiffs are persons whose wire, oral or electronic communications have been intercepted, disclosed and/or intentionally used by Defendants in violation of 18 U.S.C. § 2511(1)(a), and are authorized to recover damages and other relief in a civil action pursuant to 18 U.S.C. § 2520.

36. Defendants' violations have injured Plaintiffs, including, by way of example, depriving Plaintiffs of subscription revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, and interfering with Plaintiffs' prospective business relations.

37. Defendants violated 18 U.S.C. § 2511(1)(a) for tortious or illegal purposes, or for purposes of direct or indirect commercial advantage or private commercial gain.

38. Defendants knew or should have known that intercepting, endeavoring to intercept, and/or procuring others to intercept or endeavor to intercept Plaintiffs' encrypted satellite transmissions of television programming and control words, without authorization by Plaintiffs, was and is illegal and prohibited. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs do not have an adequate remedy at law to redress such continued violations. Unless restrained by this Court, Defendants will continue to violate 18 U.S.C. § 2511(1)(a).

**COUNT 3**

**CIRCUMVENTING A TECHNOLOGICAL MEASURE  
THAT EFFECTIVELY CONTROLS ACCESS TO A COPYRIGHTED  
WORK IN VIOLATION OF 17 U.S.C. § 1201(a)(1)**

39. Plaintiffs repeat and reallege the allegations in all preceding paragraphs as if set forth fully herein.

40. By connecting or allowing the DISH Network satellite receivers and/or access cards used by Defendants to be connected to an IKS server, distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, Defendants circumvented, and/or assisted others in circumventing, a technological measure that effectively controls access to a copyrighted work without authorization by Plaintiffs, in violation of 17 U.S.C. § 1201(a)(1).

41. Defendants' violations have injured Plaintiffs, including, by way of example, depriving Plaintiffs of subscription revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, and interfering with Plaintiffs' prospective business relations.

42. Defendants violated 17 U.S.C. § 1201(a)(1) willfully and for purposes of purposes of direct or indirect commercial advantage or private commercial gain.

43. Defendants knew or should have known that circumventing technological measures that effectively control access to a copyrighted work without authorization by Plaintiffs, was and is illegal and prohibited. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs do not have an adequate remedy at law to redress such continued violations. Unless restrained by this Court, Defendants will continue to violate 17 U.S.C. § 1201(a)(1).

**COUNT 4**

**PROVIDING ASSISTANCE IN CIRCUMVENTING A TECHNOLOGICAL  
MEASURE THAT CONTROLS ACCESS TO A COPYRIGHTED WORK  
IN VIOLATION OF 17 U.S.C. § 1201(a)(2)**

44. Plaintiffs repeat and reallege the allegations in all preceding paragraphs as if set forth fully herein.

45. By connecting or allowing Defendants' DISH Network satellite receiver and/or access card to be connected to an IKS server, distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, Defendants offered, provided or otherwise trafficked in a technology, product, service, device, component or part thereof that (1) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a copyrighted work, (2) has only limited commercially significant purpose or use other than to circumvent such technological measure, or (3) is marketed by Defendants or another acting in concert with Defendants for use in circumventing a technological measure that effectively controls access to a copyrighted work without authorization by Plaintiffs, in violation of 17 U.S.C. § 1201(a)(2).

46. Defendants' violations have injured Plaintiffs, including, by way of example, depriving Plaintiffs of subscription revenues and other valuable consideration, compromising

Plaintiffs' security and accounting systems, and interfering with Plaintiffs' prospective business relations.

47. Defendants violated 17 U.S.C. § 1201(a)(2) willfully and for purposes of purposes of direct or indirect commercial advantage or private commercial gain.

48. Defendants knew or should have known that Defendants' conduct was and is illegal and prohibited. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs do not have an adequate remedy at law to redress such continued violations. Unless restrained by this Court, Defendants will continue to violate 17 U.S.C. § 1201(a)(2)

#### COUNT 5

#### BREACH OF CONTRACT

49. Plaintiffs repeat and reallege the allegations in all preceding paragraphs as if set forth fully herein.

50. Defendants Munid and Ootra Ramkissoo entered into a Residential Customer Agreement with DISH Network that, among other things, limited Defendants' authorization to receive and view DISH Network television programming in the manner and for the purpose set forth in the Residential Customer Agreement. The Residential Customer Agreement restricts the use of DISH Network programming to "private viewing," defined as follows:

Private Home Viewing Only. DISH Network provides Services to you solely for viewing, use and enjoyment in your private home. You agree that no Services provided to you will be viewed in areas open to the public, commercial establishments or other residential locations. Services may not be rebroadcast or performed, and admission may not be charged for listening to or viewing any Services. If your Services are viewed in an area open to the public, a commercial establishment or another residential location, we may disconnect your Services and, in addition to all other applicable fees, you must pay us the difference between the price actually paid for Services and the full applicable rate for such Services, regardless of whether we have the right to distribute such Services in such other location.

51. The Residential Customer Agreement prohibits Defendants Munid and Ootra Ramkissoon from directly or indirectly using a single residential account for receiving television programming on other satellite receivers or other locations, and restricts the location of the DISH Network receiving equipment to the residential address provided by Defendants:

All of your receivers must be located at the same residence and continuously connected to the same land-based telephone line and/or broadband home network. If you wish to receive Services at two different residential locations, you must open a separate account for each location, unless otherwise specifically authorized by Dish Network. You may not directly or indirectly use a single account for the purpose of authorizing Services for multiple DISH Network receivers that are not all located in the same residence and connected to the same land-based telephone line and/or broadband home network. If we later determine that you did, we may disconnect your Services and, in addition to all other applicable fees, you agree to pay us the difference between the amounts actually received by us and the full retail price for the Services authorized for each DISH Network receiver on your account.

52. The Residential Customer Agreement prohibits Defendants Munid and Ootra Ramkissoon from tampering with the satellite receiver, access card or other components:

Proprietary Components and Software. DISH Network receivers and Smart Cards contain components and software that are proprietary to DISH Network and its licensors. You agree that you will not try to reverse-engineer, decompile or disassemble, nor will you tamper with or modify, any software or hardware contained within any receiver or Smart Card. Such actions are strictly prohibited and may result in the termination of this Agreement, disconnection of your Services and/or legal action.

53. The Residential Customer Agreement prohibits Defendants Munid and Ootra Ramkissoon from using the software and code in the satellite receiver for any purpose other than the operation of Defendants' actual satellite receiver and prohibits Defendants Munid and Ootra Ramkissoon from copying, distributing or sharing any part of it, which includes control words:

Software License. You are licensed to use the software provided in your DISH Network receiver(s), as updated by DISH Network, its licensors and/or its suppliers from time to time, solely in executable code form, solely in conjunction with lawful operation of the DISH Network receiver(s) that you purchased or leased, and solely for the purposes permitted under this Agreement. You may not copy, modify or transfer any software provided in your DISH Network receiver(s), or any copy of such software, in whole or in part. You may not reverse-engineer, disassemble, decompile or translate such software,

or otherwise attempt to derive its source code, except to the extent allowed under any applicable laws. You may not rent, lease, load, resell for profit or distribute any software provided in your DISH Network receiver(s), or any part thereof. Such software is licensed, not sold, to you for use only under the terms and conditions of this license, and DISH Network, its licensors and its suppliers reserve all rights not expressly granted to you. Except as stated above, this license does not grant to you any intellectual property rights in the software provided in your DISH Network receiver(s). Any attempt to transfer any of the rights, duties or obligations of this license is null and void. If you breach any term or condition of this license, this license will automatically terminate.

54. The Residential Customer Agreement required Defendants Munid and Ootra Ramkissoo to immediately notify DISH Network if any DISH Network equipment were removed from the residential address Defendants provided when setting up Defendants' residential account:

If any of your Equipment is stolen or otherwise removed from your premises without your authorization, you must notify our customer service center by telephone or in writing immediately, but in any event not later than three (3) business days after such removal, to avoid liability for payment for unauthorized use of your Equipment. You will not be liable for unauthorized use that occurs after we have received your notification.

55. The Residential Customer Agreement prohibits Defendants Munid and Ootra Ramkissoo from installing, reinstalling, attaching devices to or altering any DISH Network equipment provided to Defendants as a lease:

We may choose to lease certain Equipment to subscribers. Unless otherwise specified in an applicable Promotion Agreement(s), such Equipment (including without limitation, the LNBFs, but not the satellite antenna), shall at all times remain the sole and exclusive property of DISH Network, and we may provide or replace leased Equipment with new or reconditioned Equipment at any time, and upon cancellation or disconnection of your Services, remove or require the return of such Equipment. No leased Equipment provided to you by DISH Network shall be deemed fixtures or part of your real property. We may make such filings and recordings that we may consider necessary to evidence our ownership rights in such Equipment, and you agree to execute any and all documents that we may consider necessary for us to make such filings. Our ownership of such Equipment may be displayed by notice contained on it. You have no right at any time to pledge, sell, mortgage, otherwise encumber, give away, remove, relocate, alter or tamper with such Equipment, or to tamper with or alter any notice of our ownership on such Equipment. Any reinstallation, return, or change in the location of such Equipment must be performed by DISH Network at our then-current service rates. You shall not attach any electrical or other devices to, or in any way alter, any such Equipment without our prior written consent. You are responsible for preventing the loss or destruction of leased

Case 2:09-cv-06135-DRD-MAS Document 1 Filed 12/04/09 Page 15 of 20

Equipment and we recommend that such Equipment be covered by your homeowners, renters or other insurance policy.

56. The Residential Customer Agreement prohibits Defendants Munid and Ootra Ramkissoon from directly or indirectly engaging in or assisting others in any unauthorized interception or reception of any portion of DISH Network's satellite service and prohibits piracy:

#### **WARNING AGAINST PIRACY AND INFRINGEMENT**

A. **Piracy.** Receiving any portion of the Services without paying for them and/or any direct or indirect act or attempted act to engage or assist in any unauthorized interception or reception of any portion of the Services is a violation of various U.S. federal and state laws and of this Agreement. The penalties for violating such laws can include imprisonment and civil damage awards of up to \$110,000 per violation.

B. **Infringement.** Section 605(e)4 of Title 47 of the United States Code makes it a federal crime to modify Equipment to receive encrypted (scrambled) television programming without payment of required subscriptions. Conviction can result in a fine of up to \$500,000 and imprisonment for five years, or both. Any person who procures Equipment that has been so modified is an accessory to that offense and may be punished in the same manner. Investigative authority for violations lies with the Federal Bureau of Investigation. The Equipment may incorporate copyright protection technology that is protected by U.S. patents and other intellectual property rights. Use of such copyright protection technology must be authorized by DISH Network or its suppliers or licensors, and is intended for home and other limited pay-per-view uses only, unless otherwise authorized by DISH Network or its suppliers or licensors. Reverse engineering or disassembly is prohibited.

57. The Residential Customer Agreement also required Defendants Munid and Ootra Ramkissoon to immediately notify DISH Network of the address where DISH Network equipment was located:

**Physical Address/Change of Address.** When setting up your DISH Network account, you must provide us with the physical address where your Equipment will be located and your Services will be provided. A post office box does not meet this requirement. You must give us immediate notice of any change of name, mailing address, telephone number, or physical address where your Equipment is located. You may do this by notifying our customer service center by telephone or in writing at the phone number, mailing address, or e-mail address set forth at the top of this Agreement.

58. The DISH Network Residential Customer Agreement is an enforceable contract that confers legally enforceable rights to DISH Network.

59. By creating a residential subscriber account for improper purposes, and/or installing and maintaining DISH Network receiving equipment at locations or facilities not authorized by DISH Network, and/or distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, Defendants Munid and Ootra Ramkissoo have breached and are continuing to breach the DISH Network Residential Customer Agreement.

60. As a direct and proximate result of Defendants Munid and Ootra Ramkissoo's wrongful conduct, DISH Network has suffered and continues to suffer damages, including compensatory, consequential and/or restitutionary damages, in an amount to be proven at trial.

61. Defendants Munid and Ootra Ramkissoo knew or should have known that the conduct alleged herein violated the terms of the DISH Network Residential Customer Agreement and that Defendants were in breach of Defendants' obligations thereunder. Such violations have caused and will continue to cause DISH Network irreparable harm, and DISH Network does not have an adequate remedy at law to redress such continued violations. Unless restrained by this Court, Defendants Munid and Ootra Rankissoo will continue to violate the DISH Network Residential Customer Agreement.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs seek judgment against Defendants as follows:

A. Find that Defendants' conduct in creating a residential subscriber account for improper purposes, and/or installing and maintaining or allowing DISH Network receiving equipment to be installed and maintained at locations or facilities not authorized by DISH Network, and/or distributing, retransmitting and/or re-broadcasting Plaintiffs' control words

Case 2:09-cv-06135-DRD-MAS Document 1 Filed 12/04/09 Page 17 of 20

over the internet to others for their use in receiving and decrypting Plaintiffs' encrypted satellite signals, violated 47 U.S.C. § 605(a), 18 U.S.C. § 2511(1)(a), 17 U.S.C. § 1201(a), and state common laws;

B. Find further that Defendants' conduct and violations of federal and state laws was willful and malicious, for tortious and illegal purposes, and for purposes of direct or indirect commercial advantage or private commercial or financial gain;

C. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 18 U.S.C. § 2520(b)(1), 17 U.S.C. § 1203(b)(1)-(2), the DISH Network Residential Customer Agreement and state common law, enjoin and restrain Defendants, and persons or entities controlled directly or indirectly by Defendants or acting in conjunction with Defendants, from creating residential subscriber accounts for improper purposes, installing and maintaining DISH Network receiving equipment at locations or facilities not authorized by DISH Network, and distributing, retransmitting and re-broadcasting Plaintiffs' control words over the internet;

D. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 18 U.S.C. § 2520(b)(1), 17 U.S.C. § 1203(b)(1)-(2), the DISH Network Residential Customer Agreement and state common law, order Defendants to return to DISH Network all satellite receivers, access cards, and other hardware, software and components derived from or intended for the DISH Network satellite system;

E. In accordance with 47 U.S.C. § 605(e)(3)(C)(i) and (ii), award Plaintiffs the greater of (1) actual damages suffered by Plaintiffs and any profits made by Defendants that are attributable to the violations alleged herein, or (2) statutory damages of up to \$100,000 for each violation of 47 U.S.C. § 605(a);

F. In accordance with 18 U.S.C. § 2520(c)(2), award Plaintiffs the greater of (1) actual damages suffered by Plaintiffs and any profits made by Defendants as a result of the

Case 2:09-cv-06135-DRD-MAS Document 1 Filed 12/04/09 Page 18 of 20

violations alleged herein, or (2) statutory damages of whichever is the greater of \$100 per day for each violation of 18 U.S.C. § 2511(1) or \$10,000;

G. In accordance with 17 U.S.C. § 1203(c), award Plaintiffs the greater of (1) actual damages suffered by Plaintiffs and any additional profits of Defendants, or (2) statutory damages of \$2,500 per act of circumvention, device, product, component, offer, or performance of service;

H. In accordance with state common law, award DISH Network compensatory, consequential, and/or restitutionary damages, in an amount to be proven;

I. In accordance with 18 U.S.C. § 2520(b)(2) and state law, award Plaintiffs punitive damages;

J. In accordance with 47 U.S.C. § 605(e)(3)(B)(iii), 17 U.S.C. § 1203(b)(5), 18 U.S.C. § 2520(b)(3), and state common law, and in accordance with the DISH Network Residential Customer Agreement, order Defendants to pay Plaintiffs all of their reasonable attorney's fees and costs;

K. In accordance with 47 U.S.C. § 605(e)(3)(C)(i)(I), 18 U.S.C. § 2520(c)(2)(A), 17 U.S.C. § 1203(c)(1)(A), and state common law, order Defendants to (1) provide Plaintiffs a full and accurate accounting of all profits or other benefits received by Defendants as a result of the wrongful conduct described herein, (2) pay to Plaintiffs all profits or other benefits received by Defendants from the wrongful conduct alleged herein, and (3) deliver to Plaintiffs all real or personal property, money or things of value obtained by them, directly or indirectly, or acquired by them, in whole or in part, with profits or other benefits received by Defendants from the wrongful conduct alleged herein;

L. Award Plaintiffs pre- and post-judgment interest on all damages, from the earliest date permitted by law at the maximum rate permitted by law;

Case 2:09-cv-06135-DRD-MAS Document 1 Filed 12/04/09 Page 19 of 20

M. Order Defendants to preserve and provide all evidence (including electronic data) identifying all persons and/or entities involved in or assisting the operation of IKS servers and/or receiving DISH Network programming through the unauthorized receipt of Plaintiffs' control words from IKS servers; and

N. For such additional relief as the Court deems to be just and equitable.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a jury trial on all issues so triable.

Respectfully submitted,

DATED: December 4, 2009

**LEVY, EHRLICH & PETRIELLO**

By: s/ John Petriello

John Petriello (JJP-6545)  
[john@lep-lawyers.com](mailto:john@lep-lawyers.com)  
60 Park Place  
Newark, New Jersey 07102  
Telephone: (973) 854-6700  
Facsimile: (973) 596-1781

**HAGAN NOLL & BOYLE LLC**

Chad M. Hagan (*pro hac vice* pending)  
[chad.hagan@hnblc.com](mailto:chad.hagan@hnblc.com)  
David M. Noll (*pro hac vice* to be filed)  
[david.noll@hnblc.com](mailto:david.noll@hnblc.com)  
Joseph H. Boyle (*pro hac vice* to be filed)  
[joe.boyle@hnblc.com](mailto:joe.boyle@hnblc.com)  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, TX 77024  
Telephone: (713) 343-0478  
Facsimile: (713) 758-0146

**Attorneys for Plaintiffs**

**RULE 11.2 CERTIFICATION**

Pursuant to L. Civ. R. 11.2, the undersigned counsel for the Plaintiffs hereby certifies that this matter in controversy is not the subject of any other action pending in any court, or of any pending arbitration or administrative proceeding.

Case 2:09-cv-06135-DRD-MAS Document 1 Filed 12/04/09 Page 20 of 20

Dated: December 4, 2009

By: s/ John Petriello

John Petriello (JJP-6545)

john@lep-lawyers.com

LEVY, EHRLICH & PETRIELLO

60 Park Place

Newark, New Jersey 07102

Telephone: (973) 854-6700

Facsimile: (973) 596-1781

AMENDED THIS  
MODIFIÉ CE July 6, 2009 PURSUANT TO  
CONFORMÉMENT À  
☐ RULE/LA RÈGLE 26.02 (                    )  
☒ THE ORDER OF Morawetz J.  
L'ORDONNANCE DU  
DATED/FAIT LE 2 JULY 2009  
Joanne Nicoara  
LOCAL REGISTRAR Registrar, Superior Court of Justice  
SHERIFF LOCAL  
SUPERIOR COURT OF JUSTICE COUR SUPÉRIEURE DE JUSTICE

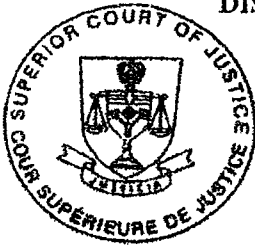
Commercial List No.: 09-CL-8091-00CL

ONTARIO  
SUPERIOR COURT OF JUSTICE  
(COMMERCIAL LIST)

BETWEEN:

DISH NETWORK LLC, ECHOSTAR TECHNOLOGIES LLC, and  
NAGRASTAR LLC

Plaintiffs



- and -

RAVINDRANAUTH RAMKISSOON a.k.a. RAVIN RAMKISSOON,  
RAVINDRANAUTH RAMKISSOON a.k.a. DIGITAL, RAVINDRANAUTH  
RAMKISSOON a.k.a. THEDIGITALSTORE, RAVINDRANAUTH RAMKISSOON c.o.b. as  
as [www.thedigitalstore.com](http://www.thedigitalstore.com), RAVINDRANAUTH RAMKISSOON c.o.b. as  
[www.nfusionteam.com](http://www.nfusionteam.com), RAVINDRANAUTH RAMKISSOON c.o.b. as [www.canadasat.com](http://www.canadasat.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.dummychat.com](http://www.dummychat.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusioncanada.com](http://www.nfusioncanada.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusioncanada.ca](http://www.nfusioncanada.ca),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusiononline.com](http://www.nfusiononline.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusionrepair.com](http://www.nfusionrepair.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusionwarrantycenter.com](http://www.nfusionwarrantycenter.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nuvenio.ca](http://www.nuvenio.ca),  
RAVINDRANAUTH RAMKISSOON c.o.b. as [www.nfusiondepo.com](http://www.nfusiondepo.com),  
RAVINDRANAUTH RAMKISSOON c.o.b. as DIGITAL R US, ANANDANAUTH  
RAMKISSOON a.k.a. ANTHONY RAMKISSOON, ROSELINE RAMKISSOON,  
DIGITAL STORE INC., E-CANADA SOLUTIONS INC., N-FUSION CANADA INC.,  
7016581 CANADA LIMITED, JOHN DOE, JANE DOE and other persons unknown who  
have conspired with the named Defendants

Defendants

AMENDED STATEMENT OF CLAIM

TO THE DEFENDANTS

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiffs. The claim made against you is set out in the following pages.

- 2 -

IF YOU WISH TO DEFEND THIS PROCEEDING, you or an Ontario lawyer acting for you must prepare a statement of defence in Form 18A prescribed by the Rules of Civil Procedure, serve it on the Plaintiffs' lawyer and file it, with proof of service, in this court office, WITHIN TWENTY DAYS after this statement of claim is served on you, if you are served in Ontario.

If you are served in another province or territory of Canada or in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period is sixty days.

Instead of serving and filing a statement of defence, you may serve and file a notice of intent to defend in Form 18B prescribed by the Rules of Civil Procedure. This will entitle you to ten more days within which to serve and file your statement of defence.

IF YOU FAIL TO DEFEND THIS PROCEEDING, JUDGMENT MAY BE GIVEN AGAINST YOU IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU. IF YOU WISH TO DEFEND THIS PROCEEDING BUT ARE UNABLE TO PAY LEGAL FEES, LEGAL AID MAY BE AVAILABLE TO YOU BY CONTACTING A LOCAL LEGAL AID OFFICE.

Date: March 23, 2009

**Christina Irwin**  
Registrar, Superior Court of Justice

JSB

Local Registrar

Address of Court Office:  
330 University Avenue  
Toronto, Ontario  
M5G 1R7

TO: RAVINDRANAATH RAMKISSOON a.k.a. RAVIN RAMKISSOON,  
RAVINDRANAATH RAMKISSOON a.k.a. DIGITAL, RAVINDRANAATH  
RAMKISSOON a.k.a. THEDIGITALSTORE, RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.thedigitalstore.com](http://www.thedigitalstore.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusionteam.com](http://www.nfusionteam.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.canadasat.com](http://www.canadasat.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.dummychat.com](http://www.dummychat.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusioncanada.com](http://www.nfusioncanada.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusioncanada.ca](http://www.nfusioncanada.ca), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusiononline.com](http://www.nfusiononline.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusionrepair.com](http://www.nfusionrepair.com), RAVINDRANAATH  
RAMKISSOON c.o.b. as [www.nfusionwarrantycenter.com](http://www.nfusionwarrantycenter.com),  
RAVINDRANAATH RAMKISSOON c.o.b. as [www.nuvenio.ca](http://www.nuvenio.ca),  
RAVINDRANAATH RAMKISSOON c.o.b. as [www.nfusiondepo.com](http://www.nfusiondepo.com),  
RAVINDRANAATH RAMKISSOON c.o.b. as DIGITAL R US  
2901 Jane Street, Unit 91  
Toronto, Ontario, M3N 2J8

- 3 -

AND TO: ANANDANAUTH RAMKISSOON a.k.a. ANTHONY RAMKISSOON  
60 Brentwood Road  
Angus, Ontario, L0M 1B0

AND TO: ROSELINE RAMKISSOON  
2901 Jane Street, Unit #91  
Toronto, Ontario, M3N 2J8

AND TO: DIGITAL STORE INC.  
34 Futurity Gate, Unit #7  
Vaughan, Ontario

AND TO: DIGITAL STORE INC.  
130 Davis Drive, Unit #6  
Newmarket, Ontario

AND TO: DIGITAL STORE INC.  
408 Dunlop Street West, #Unit 6  
Barrie, Ontario

AND TO: DIGITAL STORE INC.  
8 Strathearn Avenue, Unit #12  
Brampton, Ontario

AND TO: E-CANADA SOLUTIONS INC.  
2901 Jane Street, Suite #91  
Toronto, Ontario, M3N 2J8

AND TO: N-FUSION CANADA INC.  
119 Wanda Street  
Bradford, Ontario, L3Z 2A6

AND TO: 7016581 CANADA LIMITED  
60 Brentwood Road  
Angus, Ontario, L0M 1B0

AND TO: JOHN DOE

AND TO: JANE DOE

AND TO: Other persons unknown who have conspired with the named Defendants

- 4 -

### CLAIM

1. The Plaintiffs, Dish Network Satellite LLC, EchoStar Technologies LLC (collectively "EchoStar") and NagraStar LLC ("NagraStar"), claim as against the Defendants, Ravindranauth Ramkissoon a.k.a. Ravin Ramkissoon, Ravindranauth Ramkissoon a.k.a. Digital, Ravindranauth Ramkissoon a.k.a. THEDIGITALSTORE, Ravindranauth Ramkissoon c.o.b. as *www.thedigitalstore.com*, Ravindranauth Ramkissoon c.o.b. as *www.nfusionteam.com*, Ravindranauth Ramkissoon c.o.b. as *www.canadasat.com*, Ravindranauth Ramkissoon c.o.b. as *www.dummychat.com*, Ravindranauth Ramkissoon c.o.b. as *www.nfusioncanada.com*, Ravindranauth Ramkissoon c.o.b. as *www.nfusioncanada.ca*, Ravindranauth Ramkissoon c.o.b. as *www.nfusiononline.com*, Ravindranauth Ramkissoon c.o.b. as *www.nfusionrepair.com*, Ravindranauth Ramkissoon c.o.b. as *www.nfusionwarrantycenter.com*, Ravindranauth Ramkissoon c.o.b. as *www.nuvenio.ca*, Ravindranauth Ramkissoon c.o.b. as *www.nfusiondepo.com*, Ravindranauth Ramkissoon c.o.b. as Digital R Us ("Ramkissoon"), Anandanauth Ramkissoon a.k.a. Anthony Ramkissoon ("Anthony"), Roseline Ramkissoon ("Roseline"), Digital Store Inc. ("Digital Store"), and E-Canada Solutions Inc. ("E-Canada Solutions"), N-Fusion Canada Inc. and 7016581 Canada Limited (collectively the "Digital Store Defendants"):

- (a) an interim, interlocutory, and permanent injunction restraining the Digital Store Defendants, jointly and severally, and their officers, directors, servants, agents, employees, and any and all persons acting on behalf of or in conjunction with any of the Digital Store Defendants, and any and all persons having notice of this injunction, from directly or indirectly, by any means whatsoever:
- (b) designing, developing, marketing, selling, distributing, providing, trafficking in, exposing or offering for the purpose of trade or otherwise, any device, technology, product, service, equipment or apparatus, software, programming code, or any component thereof, which has or may be used, or is or was intended to be used, for the purpose of circumventing the Plaintiffs' security system, thereby permitting the

- 5 -

unauthorized reception and decoding of EchoStar's encrypted satellite television programming signals ("DISH Network Programming"), and services in support thereof, including, without limiting the generality of the foregoing, free-to-air receivers ("FTA receivers") programmed or modified to facilitate the theft of DISH Network Programming, FTA receivers designed to facilitate the theft of DISH Network Programming through the use of Internet Key Sharing ("IKS") / Control Word Sharing, IKS servers, DISH Access Cards (as defined herein), Bell ExpressVu Access Cards, Internet dongles, piracy software components, and services in support thereof ("Piracy Technology");

- (i) operating, maintaining, servicing, modifying, accessing, posting content or software files to, or otherwise assisting or participating in the Internet world wide web sites *www.thedigitalstore.com*, *www.nfusionteam.com*, *www.canadasat.com*, *www.dummychat.com*, *www.nfusioncanada.com*, *www.nfusioncanada.ca*, *www.nfusiononline.com*, *www.nfusionrepair.com*, *www.nfusionwarrantycenter.com*, *www.nuvenio.ca*, and *www.nfusiondepo.com* (collectively referred to as the "Web Sites") or any other web site for any purpose contrary to this injunction, or participating or engaging in any electronic mail, newsgroup, Internet relay chat communications, and forum web sites for any purpose contrary to this injunction;
- (ii) creating, modifying, operating, maintaining, servicing, accessing, or posting content to any other web site for any purpose contrary to this injunction;
- (iii) soliciting any person to purchase Piracy Technology from the Digital Store Defendants, the Web Sites or any other web site;
- (iv) advising, instructing, counselling, directing, recommending, or informing any person on the identification, purchase, acquisition or use of any Piracy

- 6 -

Technology, including the programming, modification or use of any FTA receiver for the purpose of stealing DISH Network Programming, or providing services in support of such activities; and

- (v) assisting, aiding or abetting any other person in carrying out any of the activities described in paragraphs (a)(i) to (a)(v) above;
- (c) an Order requiring the Digital Store Defendants, their officers, directors, servants, agents, employees, and any and all persons acting on behalf of or in conjunction with any of the Digital Store Defendants, and any and all persons having control of the Web Sites and any other web sites owned or operated by the Digital Store Defendants, to forthwith upon the completion of the copying by EchoStar of the Web Sites and any other web sites owned or operated by the Digital Store Defendants, their databases, and any data stored or contained therein, remove from the Web Sites and any other web sites owned or operated by the Digital Store Defendants and render inaccessible by any person any and all text, graphics, electronic data or other content of the Web Sites and any other web sites owned or operated by the Digital Store Defendants pertaining to any and all Piracy Technology, however stored, contained or held, and not subsequently post content on the Web Sites or any other web site for any purpose contrary to the terms of the Order;
- (d) an Order requiring the Digital Store Defendants, their officers, directors, servants, agents, employees and anyone else acting on their behalf, and any person(s) appearing to be in charge of the premises of the Digital Store Defendants (the "Premises") to forthwith permit entry and re-entry into the Premises to the persons authorized in the Order (the "Authorized Persons") for the purposes of searching for, identifying, inspecting, preserving, reproducing, and removing into the custody of the Independent Supervising Solicitor any and all documents, items, devices, computers, electronic media, data or equipment, and any component thereof, which are listed in

- 7 -

Schedule "A" hereto (the "Evidence") or which EchoStar's solicitors believe to be the Evidence;

- (e) an Order that upon service of the Order, the Digital Store Defendants, their officers, directors, servants, agents, employees and anyone else acting on their behalf, and any person(s) upon whom the Order is served, shall forthwith disclose to the Authorized Persons and deliver up and grant unrestricted access to the Authorized Persons to any and all of the Evidence, wherever situate, including, but not limited to:
  - (i) any and all Piracy Technology;
  - (ii) any and all IKS servers and any components thereof;
  - (iii) the whereabouts of any and all IKS servers owned, operated or used by the Digital Store Defendants or to which the Digital Store Defendants have access;
  - (iv) the Web Sites, the databases contained or stored therein, any data contained therein and any of the Evidence, and the servers on which the Web Sites reside (including by providing root level, administrative level, and any other level of access that the Digital Store Defendants may have);
  - (v) any other web site, its databases and servers, owned or operated by the Digital Store Defendants or to which the Digital Store Defendants have access containing any of the Evidence (including by providing root level, administrative level, and any other level of access that the Digital Store Defendants may have) including any electronic mail, newsgroup, Internet relay chat communications, and forum web sites;

- 8 -

- (vi) the names, addresses, e-mail addresses, telephone numbers, fictional usernames and Internet Protocol addresses of any and all of the Digital Store Defendants' customers, suppliers, coders, associates, and affiliates, and any and all of the Web Sites' users, members, and subscribers, and any and all persons who have been solicited to purchase or acquire or who have purchased or acquired any products or services from the Digital Store Defendants and the Web Sites pertaining in any way to Piracy Technology;
- (vii) any and all records of purchases, sales, or distribution of Piracy Technology, including any invoices, financial or accounting records, ledgers, books, accounts, banking records, statements, shipping documents, web site databases, and online payment processor or auction accounts (including PayPal and eBay), which disclose the nature, volume, and extent of the Digital Store Defendants' dealings in Piracy Technology; and
- (viii) the whereabouts of all of the Evidence, whether under the possession, custody or control of the Digital Store Defendants or any third party;
- (f) damages in the amount of \$10,000,000.00 for breaches of the *Radiocommunication Act*, copyright infringement, conspiracy, conversion, unlawful interference with economic relations, and unjust enrichment;
- (g) an accounting of all profits from the Digital Store Defendants' wrongful activities;
- (h) an equitable tracing of the proceeds from the Digital Store Defendants' wrongful activities into the assets, property, and interests of the Digital Store Defendants, as defined below;

- 9 -

- (i) a declaration that the Plaintiffs possess an equitable interest in the real and personal property of the Digital Store Defendants, on the basis of a constructive, resulting, implied and/or express trust, the particulars of which will be provided prior to trial;
- (j) the issuance of a certificate of pending litigation over the lands and premises municipally known as 119 Wanda Street, Bradford, Ontario, L3Z 2A3, which are legally described as "PT LT 7 PL 848, as in RO1379220; Bradford-WGW" (the "Wanda Property");
- (k) aggravated, exemplary, and punitive damages;
- (l) special damages, the particulars of which will be provided prior to trial;
- (m) an Order that the Court file in this action shall be sealed for ten (10) days from the date of the Order and all of the materials filed and to be filed in these proceedings shall be secured by the Registrar during that period of time, and the public shall not be granted access to the Court file or any materials therein during that period of time without an Order of the Court;
- (n) pre-judgment and post-judgment interest in accordance with the *Courts of Justice Act*, R.S.O. 1990, c. C.43, as amended;
- (o) the costs of this action on a substantial indemnity scale, plus GST; and
- (p) such further and other relief as this Honourable Court may deem just.

- 10 -

2. The Plaintiffs claim, as against the Defendants John Doe, Jane Doe, and other persons unknown who have conspired with the Digital Store Defendants (the "Co-Conspirators"):

- (a) an interim, interlocutory, and permanent injunction restraining each of the Co-Conspirators, jointly and severally, and their officers, directors, servants, agents, employees and anyone else acting on their behalf or in conjunction with them or any and all persons with notice of this injunction, from directly or indirectly, by any means whatsoever:
  - (i) designing, developing, marketing, selling, distributing, providing, trafficking in, exposing or offering for the purpose of trade or otherwise Piracy Technology;
  - (ii) operating, maintaining, servicing, modifying, accessing, posting content to, or otherwise assisting or participating in the Web Sites, or any other web site for any purpose contrary to this injunction, or participating or engaging in any electronic mail, newsgroup, Internet relay chat communications, internet key sharing and forum web sites for any purpose contrary to this injunction;
  - (iii) creating, modifying, operating, maintaining, servicing, accessing, or posting content to any other web site for any purpose contrary to this injunction;
  - (iv) soliciting any person to purchase Piracy Technology from the Digital Store Defendants, the Web Sites or any other web site;
  - (v) advising, instructing, counselling, directing, recommending, or informing any person on the identification, purchase, acquisition or use of any Piracy Technology, including the programming, modification, or use of any FTA receiver for the purpose of stealing DISH Network Programming, or providing services in support of such activities; and

- 11 -

- (vi) assisting, aiding or abetting any other person in carrying out any of the activities described in paragraphs 2(a)(i) to 2(a)(v) above;
- (b) an Order requiring the Co-Conspirators to deliver up, grant access to and disclose to the Plaintiffs the whereabouts of any and all Piracy Technology in their possession, power, or control;
- (c) damages for breaches of the *Radiocommunication Act*, copyright infringement, conspiracy, conversion, unlawful interference with economic relations and unjust enrichment;
- (d) an accounting of profits for the profits made from the Co-Conspirators' wrongful activities;
- (e) aggravated, exemplary, and punitive damages;
- (f) special damages, the particulars of which will be provided prior to trial;
- (g) an Order that the Court file in this action and all of the materials filed or to be filed in this action, including any interim or interlocutory proceedings herein shall be sealed and the public shall not be granted access to said file or materials without an Order of this Court;
- (h) pre-judgment and post-judgment interest in accordance with the *Courts of Justice Act*, R.S.O. 1990, c. C.43, as amended;
- (i) the costs of this action on a substantial indemnity scale, plus GST; and
- (j) such further and other relief as this Honourable Court may deem just.

- 12 -

#### THE PARTIES

3. EchoStar is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. Dish Network is licensed by the U.S. Federal Communications Commission to broadcast its services in the United States. EchoStar uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment programming services to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price). EchoStar Technologies LLC is incorporated under the laws of the States of Colorado and Texas, with its principal place of business at 100 Inverness Circle East, Englewood, Colorado. Dish Network is incorporated under the laws of the States of Colorado and Texas, with its principal place of business at 9601 South Meridien Blvd., Englewood, Colorado.
4. EchoStar operates its DBS service under the trade name "DISH Network". More than thirteen million household and commercial viewers of DISH Network can obtain hundreds of channels of programming in digital video and CD-quality audio. EchoStar electronically scrambles its satellite transmission to prevent unauthorized viewing of DISH Network Programming. EchoStar, together with its affiliates, employs over 20,000 people.
5. EchoStar purchases the distribution rights for most of the DISH Network Programming it sells from program providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other programming rights holders. EchoStar contracts and pays for the right to distribute DISH Network Programming to its subscribers, and holds rights to exhibit the DISH Network Programming to them.
6. EchoStar is not licensed by the Government of Canada to permit the descrambling of its scrambled subscription programming signals in Canada at present. At this time, no one has the lawful right (*i.e.*, the regulatory, contractual and copyrights necessarily pertaining to the content of

- 13 -

the scrambled programming signal transmitted by EchoStar) to descramble, authorize or facilitate the descrambling of EchoStar's signal in Canada.

7. NagraStar is a supplier of proprietary technology, including components that are part of a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"), which is used by EchoStar to scramble its satellite signals. NagraStar is a joint venture between EchoStar Corporation and the Kudelski Group, a group of companies headquartered in Switzerland. NagraStar provides DNASP to EchoStar under a licence from the Kudelski Group.

8. The Defendant, Ramkissoon, is an individual who resides in Ontario and a co-owner of the Wanda Property. At all material times, Ramkissoon carried on business as the Web Sites, and the Digital Store, Digital R Us, E-Canada Solutions Inc. and N-Fusion Canada Inc. Ramkissoon is or was, at all material times, the sole director, principal and directing mind of the Defendants, Digital Store, Digital R Us, E-Canada Solutions Inc. and N-Fusion Canada Inc. and was actively involved in and/or had personal knowledge of its their unlawful activities, as described herein, and as such is personally liable for its their acts and omissions.

9. The Defendant, Anthony, is an individual residing in Ontario who, at all material times and is was an employee of the Digital Store. Anthony is also the sole officer, director, principal and directing mind of 7016581 Canada Limited. At all material times, Anthony sold and distributed Piracy Technology and otherwise assisted, aided and abetted the activities of the Digital Store Defendants as described herein. Anthony was actively involved in and/or had personal knowledge of the unlawful activities of the Digital Store Defendants as described herein, and as such is personally liable for their acts and omissions.

10. The Defendant, Roseline (sometimes referred to as Rosaline Ramkissoon), is an individual residing in Ontario and a co-owner of the Wanda Property. Roseline is also the sole officer, director, principal and directing mind of N-Fusion Canada Inc. At all material times, Roseline sold and distributed Piracy Technology and otherwise assisted, aided and abetted the activities of the Digital Store Defendants as described herein. Roseline was actively involved in and/or had personal

- 14 -

knowledge of the unlawful activities of the Digital Store Defendants as described herein, and as such is personally liable for their acts and omissions.

11. The Defendant, Digital Store, is a corporation incorporated under the laws of Ontario.

12. The Defendant, E-Canada Solutions, is a corporation incorporated under the laws of Ontario, with a registered office address of 2901 Jane Street, Suite #91, Toronto, Ontario, M3N 2J8 (the "Jane Street Address"). Ramkissoo resides at the Jane Street Address.

13. The Defendant, N-Fusion Canada Inc., is a corporation incorporated under the laws of Ontario, with a registered office address of 119 Wanda Street, Bradford, Ontario, L3Z 2A6.

14. The Defendant, 7016581 Canada Limited, is a corporation incorporated under the laws of Ontario, with a registered office address of 60 Brentwood Road, Angus, Ontario, L0M 1B0.

15. The Co-Conspirators are persons, the identity of whom is unknown to the Plaintiffs but known to the Digital Store Defendants, who have unlawfully created, designed, developed, manufactured, supplied, trafficked in, offered for sale, sold, used, purchased and acquired Piracy Technology and/or facilitated the unauthorized reception of DISH Network Programming, without authorization from or payment to EchoStar, including but not limited to customers, suppliers, coders, associates, and affiliates of the Digital Store Defendants.

#### THE DISH NETWORK

16. EchoStar has invested several billion U.S. dollars to develop and deploy its distribution and broadcasting system. All programming distributed by EchoStar is delivered to one or more of its broadcast centers in Wyoming, Arizona and elsewhere, where it is digitized, compressed, and scrambled. EchoStar then transmits the scrambled signals to multiple satellites located in geosynchronous orbit above the Earth.

- 15 -

17. EchoStar's satellites have relatively fixed "footprints" (i.e., a terrestrial territory within which the scrambled satellite broadcast signals can be received). The "footprints" of the satellites used by EchoStar cover the United States, portions of Mexico, parts of Canada, and several Caribbean nations and territories. The satellites relay the scrambled signals back to Earth, where they can be received by EchoStar's subscribers.

18. In order to receive DISH Network Programming, a consumer must obtain certain satellite system hardware consisting primarily of: (1) a satellite dish, (2) an integrated receiver/decoder (also called a "receiver", "IRD" or a "set-top box"), and (3) a DISH Network "access card" (sometimes referred to as a "smart card") ("DISH Access Card") (collectively, the "Receiving Equipment"). In certain newer receivers, the DISH Access Card microprocessor technology is built directly into the receiver and the receiver is "cardless". This built-in technology is included in the term DISH Access Card.

19. Satellite dishes can be mounted on a rooftop, deck railing or other structure at the subscriber's home or business. The signal is received by the dish and transmitted by wire to the receiver. The receiver processes and descrambles the incoming signal using the credit-card sized DISH Access Card. The DISH Access Card is loaded into the receiver through a slot in the unit. EchoStar subsidizes the cost of the Receiving Equipment in anticipation of revenues that will be received from subscribers to DISH Network Programming.

20. The DISH Access Card is essential to the operation of the receiver because it contains a secure embedded microprocessor component that functions as a small security computer, with secret keys, also known as box keys ("Box Keys"), and software code containing descrambling technology that communicates with the receiver and enables the descrambling of DISH Network Programming (the "DISH Software"). The DISH Software and the security software contained in the receiver is licensed from NagraStar which regards it as a trade secret and strictly confidential information that it would not disclose to any third party.

- 16 -

21. Without a subscription, EchoStar does not authorize access to its scrambled programming. EchoStar provides the DISH Access Cards to its subscribers for use with the receivers for the sole purpose of enabling authorized access to the DISH Network Programming. The DISH Access Cards are the property of EchoStar that must be returned to EchoStar on request. Any modification of or tampering with the DISH Access Card is prohibited by EchoStar. Moreover, the terms on which DISH Access Cards are made available to consumers provide that they are strictly non-transferable.

#### **THE ECHOSTAR SECURITY SYSTEM**

22. Because EchoStar generates revenues through sales of subscription packages and pay-per-view programming, and because its ability to attract and retain distribution rights for copyrighted programming is dependent upon preventing the unauthorized descrambling of its signals, all of EchoStar's video channels, except for certain promotional channels, are digitally encoded and scrambled to prevent unauthorized viewing. NagraStar similarly generates its revenues by ensuring the integrity of the scrambling technology it sells, including DNASP. Accordingly, EchoStar and NagraStar devote substantial resources to the continuing development and improvement of their security system.

23. The security system uses a complex encryption system that is combined with a scrambler/encoder system to form EchoStar's rights management and security system (the "EchoStar Security System"), which, among other things, protects DISH Network Programming from being viewed by unauthorized persons.

24. The EchoStar Security System serves two interrelated functions: (1) subscriber rights management, which allows EchoStar to "turn on" or "turn off" programming that a customer has ordered, cancelled or changed; and (2) scrambling, which prevents individuals or entities who have not ordered DISH Network Programming from viewing it.

25. NagraStar provides EchoStar with DISH Access Cards that are programmed and serialized (*i.e.*, assigned unique electronic identifying numbers). EchoStar then provides the DISH Access

- 17 -

Cards to receiver manufacturers, who include one DISH Access Card with each receiver (unless the receiver is "cardless").

26. Upon the first activation of a customer's subscription, EchoStar sends a signal to the DISH Access Card in order to "pair" the DISH Access Card to the customer's receiver. Both the DISH Access Card and the receiver have a unique identification number that is maintained by EchoStar's subscriber management system. This pairing operation, using the two unique identification numbers and their associated Box Keys, is mandatory for the proper operation of the EchoStar Security System. Before being "paired", a DISH Access Card cannot be legally used with any receiver, and after "pairing", the DISH Access Card can only be used with that specific receiver and the receiver can only be used with that specific DISH Access Card. In addition, in order to descramble DISH Network Programming, the identification numbers and Box Keys must also be "paired" with other keys transmitted by EchoStar in its satellite signal datastream.

27. The DISH Access Card, in conjunction with the receiver, is programmed to handle secure telecommunications over telephone lines with respect to viewer purchases of pay-per-view movies or other events. These communications are essential to EchoStar's billing, accounting, security, and customer service. To enable these telecommunications, EchoStar directs DISH Network subscribers to connect their receiver to a telephone line.

28. The DISH Access Card (including the equivalent technology built into newer receivers) is therefore fundamental to the EchoStar Security System in that it prevents unauthorized program viewing, while permitting authorized receivers used by EchoStar's subscribers to descramble the signals and permit program viewing in accordance with the subscriber's authorized subscription package and pay-per-view purchases.

- 18 -

**THE BLACK MARKET IN PIRACY TECHNOLOGY, ILLEGALLY-MODIFIED DISH ACCESS CARDS  
AND PROGRAMMING SERVICES, AND ECHOSTAR'S EFFORTS TO COMBAT PIRACY**

29. In late 1998, rumours began to circulate that "hackers" were compromising the EchoStar Security System so that they could receive and descramble DISH Network Programming without authorization from EchoStar. Subsequent investigations confirmed these rumours to be true. The persons who are engaged in or connected with businesses which were engaged in various aspects of satellite television piracy or who otherwise participated in the piracy community are hereinafter referred to as "Pirates".

30. Various types of equipment and devices began to appear on the market for the sole purpose of illegally descrambling or "pirating" DISH Network Programming. These devices initially consisted of printed circuit boards that when programmed, operated in the place of, and/or in conjunction with, DISH Access Cards. These devices compromised the EchoStar Security System by modifying and/or circumventing the security software in the DISH Access Cards.

31. EchoStar uses the same technological platform (i.e., receivers and access card encryption technologies) as Bell ExpressVu Limited Partnership ("ExpressVu"), a Canadian-based provider of encrypted satellite television programming services ("ExpressVu Programming"). Accordingly, the same piracy devices can often be used to steal DISH Network Programming and ExpressVu Programming. In fact, Pirates have even modified certain versions of DISH Access Cards steal ExpressVu Programming and vice versa.

32. EchoStar's anti-piracy strategy includes the periodic introduction of new generations of DISH Access Cards containing updated software that Pirates have not yet hacked. The first DISH Access Card was known as the ROM 2 card. EchoStar and NagraStar subsequently deployed DISH Access Cards with improved anti-piracy technologies, including the ROM 3, ROM 10, ROM 11, ROM 101, ROM 102, ROM 103, ROM S01, ROM S02, ROM 206 and ROM 241. Pirates often refer to the ROM 101 and later DISH Access Cards as the "Nagra 2" or "N2" system.

- 19 -

33. EchoStar is currently transitioning its subscribers to a new generation of DISH Access Cards known as the ROM 241 containing updated software that Pirates have not hacked. ExpressVu has already transitioned its subscribers to the ROM 240 which, together with the ROM 241, Pirates refer to as the "Nagra 3" or "N3" system.

34. The main purpose of developing and introducing successive generations of DISH Access Cards is to foil hackers and render obsolete existing piracy devices. Converting EchoStar customers to new generations of DISH Access Cards and switching the satellite datastream so that it can only be received by the new DISH Access Cards requires the Pirates to start over again in attacking the technology. EchoStar and NagraStar have invested and continue to invest significant time and money in these enhancements. EchoStar and NagraStar also update the DISH Access Cards to improve their functionality and service to EchoStar's customers.

35. EchoStar and NagraStar also invest heavily in developing and deploying countermeasures to maintain the integrity of the EchoStar Security System, as well. Such countermeasures include electronic countermeasures ("ECM's"), which are periodically broadcast over the satellite signal datastream (sometimes referred to by Pirates as "the stream") to disable unauthorized DISH Access Cards.

36. Piracy software is an essential component of most piracy devices. Among the software offered on piracy web sites today is software that is created and offered solely for the purpose of "programming", "cracking", "flashing", "glitching", and "modifying" DISH Access Cards, receivers, or piracy devices; "repairing", "patching", "fixing" or "updating" illegally-modified DISH Access Cards, receivers, or piracy devices that have been disabled by ECM's; and "blocking" ECM's from attacking illegally-modified DISH Access Cards (so-called "blockers"). This software is known by such names as "NagraEdit", "f040", "BAPA\_BELL", "ROM Tier Maker", "jeepers", "Nagramaster", "N2Edit", "jkeys", "keygrabber", "romripper", "Enigma Edit", "Rebel Serf", and "Nagra2Elite".

37. Pirates often refer to the satellite television industry by the acronym "DSS" for "digital satellite system". Pirates also often refer to the use of modified DISH Access Cards or piracy

- 20 -

devices as "testing" (*i.e.*, implying that they are used for the purpose of "testing" the Receiving Equipment) and sometimes refer to themselves as "testers" and piracy as a "hobby". EchoStar does not authorize anyone to modify, alter, reprogram or "test" its Receiving Equipment for any purpose whatsoever. Legitimate subscribers to EchoStar would have no reason to "test", tamper with, or alter the Receiving Equipment. Rather, the sole purpose of such activities would be to circumvent the EchoStar Security System to steal DISH Network Programming.

38. Some piracy devices are sold pre-programmed with piracy software. However, in an effort to avoid prosecution, many Pirates offer only "unprogrammed" or "unflashed" piracy devices for sale to consumers. In such cases the Pirates will suggest that the piracy devices they offer for sale are "legitimate" or "legal" because the purchaser must obtain piracy software from other sources and program them before they can be used for piracy. Pirates will generally refer their customers to sources of software components either verbally, by e-mail or by way of links to software providers' web sites. This has led to a proliferation of web sites offering piracy software files for download that often restrict access to piracy software to persons who pay fees to become "members" or "subscribers" (so-called "private software" and "private sites").

39. Many Pirates also offer services in support of the piracy devices and the piracy software that they sell. These services include:

- (a) access card programming services by which DISH Access Cards are re-programmed by Pirates to permit them to be used for piracy purposes;
- (b) box key "extraction" services by which Box Keys are obtained from receivers, to be used in "pairing" the receivers to DISH Access Cards supplied by Pirates; and
- (c) "unlocking" services by which receivers and DISH Access Cards that have been "paired" together can be "unlocked", thereby permitting the receiver or DISH Access Card to be used with a DISH Access Card or receiver other than the one to which it has been "paired".

40. The ongoing provision of new versions of piracy software and the aforementioned services result in continual losses for EchoStar.

- 21 -

41. The black market in Piracy Technology represents a multimillion-dollar industry in Canada and the United States. The Pirates who fuel this black market are geographically dispersed and typically operate individually or within a very small group. By using the Internet, Pirates are able to operate without regard to national borders and reach millions of potential customers. The identities of Pirates who develop, manufacture, and distribute Piracy Technology are known only to a few. Locating their places of business and linking piracy web sites to the Pirates who operate them is often difficult.

42. Pirates are generally aware of the illegal nature of their activities, and often take steps to avoid detection and to conceal the evidence of their wrongdoing. Pirates who operate Internet-based businesses benefit from the anonymity which the Internet provides, and typically use fictitious "nicknames" in their online activities, register their web sites using false names and addresses, locate the servers containing their web sites' databases in undisclosed (and sometimes offshore) locations, and use third party on-line payment processors that store their sales records elsewhere (and sometimes offshore). Pirates can access their web sites by "remote access" from their residences and anywhere else with an Internet connection, and need not operate from conventional business premises.

#### **THE USE OF FREE-TO-AIR (FTA) RECEIVERS FOR SATELLITE PIRACY**

##### **(i) Traditional FTA Receivers**

43. In 2003, Pirates developed a new way to steal DISH Network Programming by using FTA receivers that had been programmed with piracy software.

44. FTA receivers were originally designed to receive "free-to-air" satellite television signals, which are either not scrambled or scrambled but available free of charge. There are numerous "free-to-air" television channels available in Canada and the United States, which typically offer specific ethnic, religious, business, music, information and advertisement programming. "Free-to-air" channels and FTA receivers have existed for many years, and are today manufactured and sold by

- 22 -

several companies under various brand names including "Fortec", "Pansat", "Coolsat", "Dreambox", "Coship", "Viewsat", "Freotech", "Sonicview", "Topfield", and, most recently, "nFusion" and "Captain".

45. FTA receivers are similar to the receivers used by EchoStar in that they are a set-top box, approximately the size of a DVD player, which contain descrambling circuits and software that enables them to perform their function. Some FTA receivers also contain an access card reader.

46. EchoStar and NagraStar have determined that FTA receivers are today widely used for piracy purposes, and that the market for FTA receivers increased dramatically in or around 2003, when Pirates began selling FTA receivers modified with piracy software to steal DISH Network Programming.

47. Initially, Pirates acquired FTA receivers from their manufacturers and loaded piracy software onto the circuit chips contained within them so as to mimic a DISH Access Card. This form of piracy is known as "Smart Card Emulation". EchoStar and NagraStar believe that the "coders" (i.e., software programmers) who create the piracy software gain access to a part of EchoStar's encrypted datastream that contains the "keys" (also known as the "Control Word") used to scramble and descramble the DISH Network Programming. The coders thereafter embed these keys in the piracy software, which, when loaded onto the FTA receiver, gives it the capability of descrambling DISH Network Programming without authorization from or payment to EchoStar.

48. To combat Smart Card Emulation, NagraStar and EchoStar develop and deploys ECMs that serve to either (a) change the keys used to descramble DISH Network Programming, or (b) create another layer of security that the piracy software cannot circumvent. When the Smart Card Emulation ceases to function, Pirates sometimes say that the "Autoroll" is not working. Autoroll is the capability of the piracy software to obtain continual access to keys from EchoStar's datastream. Unfortunately, these ECMs are short-term solutions because the coders usually develop and release new piracy software (sometimes called a "fix" or "update") that gives the FTA receivers the

- 23 -

capability of once again descrambling DISH Network Programming without authorization from or payment to EchoStar.

**(ii) Enhanced FTA Receivers**

49. More recently, Pirates have begun selling certain brands of FTA receivers that are capable of obtaining piracy software and "keys" to descramble DISH Network Programming directly from the Internet.

50. Once piracy software is loaded onto these FTA receivers, the Internet connection serves two piracy-related functions:

- (a) Emulation Updates: The Internet connection automatically updates the piracy software in the FTA receiver. When new piracy software is released, such as a "fix" or "update" to overcome the most recent ECM, it can be loaded directly from the Internet without the need to connect the FTA receiver to a computer. With this capability, the end-user merely responds "yes" to an on-screen prompt and the new piracy software will be downloaded and installed on the FTA receiver; and
- (b) Internet Key Sharing / Control Word Sharing: The FTA receiver contacts a server (the "IKS server") over the Internet, which responds by providing the decrypted Control Word. The IKS server has the ability to decrypt the Control Word because it is connected to legitimate subscribed ExpressVu Access Cards or legitimately subscribed or "hacked" DISH Access Cards at the server location that decrypts the Control Word. An IKS server typically consists of multiple FTA receivers connected together, each of which is responsible for descrambling specific channels.

51. The FTA receivers that support Emulation Updates and IKS, including the nFusion-brand and Captain-brand, pose unique threats to EchoStar and NagraStar for two primary reasons.

- 24 -

52. First, unlike traditional FTA receivers modified for piracy, which require Pirates to generate a "fix" or "update" following an ECM, and then require Pirates or end-users to manually program it onto each FTA receiver affected by an ECM, these FTA receivers are designed to obtain all the information they need to descramble DISH Network Programming (including all "fixes" and "updates") directly from the IKS server via the Internet. These FTA receivers can thereby automatically "recover" from ECMs and operate continuously to steal DISH Network Programming. Pirates often boast that these FTA receivers "never go down".

53. Second, because these FTA receivers rely on the IKS server, they are able to descramble DISH Network Programming even after the completion of the transition to the "Nagra 3" or "N3" generation of DISH and ExpressVu Access Cards, which will disable other piracy devices and piracy software that function only with the "Nagra 2" or "N2" generation of DISH and ExpressVu Access Cards. For this reason, these FTA receivers effectively circumvent the security enhancements contained in the "Nagra3" or "N3" generation of DISH and ExpressVu Access Cards. Pirates often boast that these FTA receivers "support N3" or are the only FTA receivers that "work with N3".

54. These FTA receivers are therefore extremely threatening to EchoStar and NagraStar's anti-piracy efforts.

55. The nFusion-brand of FTA receiver ("nFusion FTA receiver") can be directly connected to the Internet using a built-in "Ethernet" port and standard cable. The nFusion FTA receiver is sold with software to provide a so-called "IPVR" (Internet Personal Video Recorder) capability that permits it to receive free-to-air channels and, using a home or office network, record the programming on a computer hard drive to be played back at a later time. This software provides nFusion FTA receivers with a non-piracy related reason to have a built-in Ethernet port. However, EchoStar and NagraStar believe that the Ethernet connection built into the nFusion FTA receivers that facilitate connecting to the Internet was designed for and is primarily used to connect to an IKS server for the purpose of stealing DISH Network and ExpressVu programming.

- 25 -

56. Other brands of FTA receivers cannot be directly connected to the Internet because they do not have a built-in "Ethernet" port. However, Pirates sell devices known as Internet "Dongles" ("Dongles") that permit these FTA receivers to connect to the Internet using their built-in USB port and the Dongle, and thereby access an IKS server for piracy purposes. The Dongles contain a specific web server address within their flash memory to access the IKS server. As such, once the FTA receiver is loaded with piracy software (which sometimes has the word "dongle" in the filename), the Dongle is ready to be used for piracy purposes. Pirates claim that the Dongle has a legitimate purpose because it can be used with FTA receivers to obtain weather forecasts from the Internet. However, EchoStar and NagraStar believe that the primary purpose of the Dongle is to permit FTA receivers to be connected to an IKS server for piracy purposes.

57. The Captain-brand FTA receiver ("Captain FTA receiver") is marketed with a "Captain Dongle" that permits it to connect to the Internet and an IKS server for piracy purposes. Unlike nFusion FTA receivers, Captain FTA receivers are not sold with any "IPVR" software and EchoStar and NagraStar are not aware of any legitimate reason for a Captain FTA receiver to be connected to the Internet.

58. Legitimate FTA receivers do not require software to be downloaded from the Internet in order to receive FTA programming.

**(iii) FTA Piracy Accessories**

59. Pirates also sell devices known as "8PSK" modules or "DN" modules. These devices enable FTA receivers to receive so-called "MPEG-4"-format High Definition programming broadcast by EchoStar. This "MPEG-4" format is not used by ExpressVu. As such, there is no legitimate purpose for the use of these devices in Canada, and any such use is indicative of piracy of DISH Network Programming.

60. Pirates also sell digital video broadcast ("DVB") cards that can be used to view free-to-air channels on a computer. As with FTA receivers, DVB cards have a legitimate use. However, DVB

- 26 -

cards can also be used to steal DISH Network Programming. In order to use DVB cards for piracy purposes, it is necessary to install the DVB card in a computer and connect the computer to a satellite dish, cable modem or antenna. The computer is then loaded with piracy software which, in conjunction with the DVB card, permits the computer to receive and descramble DISH Network Programming. Pirates often market DVB cards as "free-to-air for your computer" and either provide the piracy software or direct their customers to web sites offering piracy software for download.

**(iv) Impact of FTA Receivers on Satellite Piracy**

61. The modification and use of FTA receivers for piracy purposes, and the equipment and devices sold in support of this purpose, represents a serious threat to EchoStar and NagraStar. The purchaser of an FTA receiver can run any software that he or she wishes on the FTA receiver. Because FTA receivers are not manufactured or sold by EchoStar and NagraStar to receive DISH Network Programming, these companies have no control over the software contained in them. As a result, security measures such as ECM's transmitted by EchoStar and NagraStar through their satellite datastream may have no effect on modified FTA receivers. EchoStar and NagraStar may therefore be unable to attack or disable modified FTA receivers in the same way that they can with EchoStar receivers that are being modified for piracy purposes. This is particularly true for IKS compatible FTA receivers, which are able to recover automatically from ECM's and are essentially unaffected by the transition to the "Nagra3" system of DISH and ExpressVu Access Cards.

62. In addition, because FTA receivers and the use of them are legal, in certain circumstances, in Canada and the United States, they are attractive to Pirates as a "legal" product with which to engage in piracy activities. This cloak of legitimacy presents serious challenges to EchoStar and NagraStar in their enforcement activities.

63. In order to avoid liability, Pirates today rarely load piracy software directly onto the FTA receivers they sell in their stores or on their web sites. Instead, they assist their customers in engaging in piracy by:

- 27 -

- (a) distributing FTA receivers and other technology, including Dongles, that are manufactured and/or designed and/or programmed for use with IKS technology to allow for the unauthorized descrambling of DISH Network Programming;
- (b) creating and distributing piracy software for FTA receivers to their customers, including by e-mail attachments or electronic storage media;
- (c) directing their customers to piracy web sites where the piracy software is available, often with the Pirates subsidizing these sites by paying for advertising on them, and often with the Pirates utilizing web site "hyperlinks" back and forth between their web sites and the piracy web sites;
- (d) selling FTA receivers and directing their customers to "installers" who either:
  - (i) program the customer's FTA receiver with piracy software;
  - (ii) deliver piracy software to the customer for the customer to program onto the FTA receiver; or
  - (iii) direct the customer to any of the numerous web sites that offer piracy software for download; and
- (e) selling or distributing peripheral devices which are of assistance in the unauthorized interception of DISH Network Programming, such as satellite dishes with "circular" LNB's (Low Noise Blockers) that will only receive signals of the encrypted, pay satellite services such as DISH Network.

#### **"FORUM" AND CHAT WEB SITES**

64. Many Pirates operate or participate in piracy web sites that serve as a "forum" for the dissemination and exchange of information pertaining to Piracy Technology and satellite piracy generally. In many cases, forum sites do not sell any Piracy Technology themselves. Rather, they:

- (a) provide information and instructions on Piracy Technology, including sources of supply, product information, and product reviews;
- (b) provide discussion threads on topics of interest to the piracy community, including software "hacks" and "fixes" designed to restore functionality to DISH Access Cards that have been disabled by ECM's;
- (c) provide "keys" for EchoStar and ExpressVu, which are required in order to unscramble programming;

- 28 -

- (d) provide piracy software files for download to their users;
- (e) provide links to and advertisements for other piracy web sites that sell Piracy Technology and related services; and
- (f) generally serve as a "community" for the exchange of information designed to permit consumers to unlawfully receive DISH Network Programming, and to permit Pirates to communicate with one another on matters of general interest.

65. Forum sites often generate revenue through the sale of memberships and advertising revenue from other piracy web sites that place advertisements or links on them. They may also accept donations from their users.

66. In some cases, Pirates operate forum sites to establish credibility in the piracy community and obtain a loyal group of users. Successful forum sites can have tens of thousands of members. The Pirates who operate forum sites sometimes designate certain users as "administrators" or "moderators" and give them authority to manage the messages posted on the forum site.

#### **ACTIONS OF THE DIGITAL STORE DEFENDANTS**

67. The Digital Defendants have been engaged, and continue to be engaged, in the sale and distribution of FTA receivers and other Piracy Technology, and services and information designed to facilitate the theft of DISH Network Programming.

68. The purpose of the Digital Store Defendants' business and undertaking dealing in Piracy Technology is to facilitate the unauthorized reception of DISH Network Programming contrary to the laws of Canada and the United States, and in reckless disregard for EchoStar's rights. In particular, the Digital Store Defendants have, among other things:

- (a) sold various brands of FTA receivers including nFusion brand FTA receivers;
- (b) sold "8PSK" modules which are designed to permit nFusion FTA receivers to receive high-definition DISH programming;

- 29 -

- (c) arranged for the release of piracy files for nFusion FTA receivers on the piracy forum web site *www.completefta.com*;
- (d) developed the nFusion FTA receivers to be connected to the Internet and access IKS servers;
- (e) promoted the nFusion FTA receivers for use with piracy files downloaded directly from the Internet;
- (f) advertised Digital Store on known piracy web sites; and
- (g) assisted, aided, and abetted other persons in carrying out piracy activities to steal DISH Network Programming.

69. As a result of these activities, the Digital Store Defendants have contravened the *Radiocommunication Act*, infringed the Plaintiffs' copyrights, conspired against EchoStar to deprive EchoStar of subscription and pay-per-view revenues and other consideration, converted EchoStar's proprietary rights unto themselves, unlawfully interfered with EchoStar's economic relations, and been unjustly enriched. All of the Digital Store Defendants' activities have been done without the authorization of the Plaintiffs and without payment or compensation to the Plaintiffs.

**THE DEFENDANTS ARE LIABLE TO THE PLAINTIFFS FOR THEIR WRONGFUL ACTS**

**(i) Breaches of the Radiocommunication Act**

70. The purpose and intended use of the Piracy Technology sold by the Digital Store Defendants is to permit the unauthorized reception of EchoStar's subscription programming signals otherwise than in accordance with authorization from the lawful distributor of that signal, contrary to section 9(1)(c) of the *Radiocommunication Act*.

- 30 -

71. The Digital Store Defendants and the Co-Conspirators have therefore been engaged in distributing, offering for sale, selling, installing, modifying, operating or possessing Piracy Technology, without lawful excuse, under circumstances that give rise to a reasonable inference that the Piracy Technology has been used, or is or was intended to be used, for the purpose of contravening section 9(1)(c) of the *Radiocommunication Act*, contrary to subsection 10(1)(b) of that statute.

72. The Digital Store Defendants have also assisted, facilitated, promoted, aided and abetted the decoding of an encrypted subscription programming signal by the Co-Conspirators, otherwise than in accordance with lawful authorization from the lawful distributor of that signal, contrary to section 9(1)(c) of the *Radiocommunication Act*, section 34(2) of the *Interpretation Act*, R.S.C. c. I-23, as amended ("*Interpretation Act*"), and section 21 of the *Criminal Code*, R.S.C. 1985, c. C-46, as amended ("*Criminal Code*").

73. As the holder of an interest in the content of a subscription programming signal, EchoStar has a civil cause of action against the Digital Store Defendants and the Co-Conspirators pursuant to section 18(1)(a) of the *Radiocommunication Act* for the loss and damage it has sustained as a result of the Digital Store Defendants' and the Co-Conspirators' activities. Accordingly, the Digital Store Defendants and the Co-Conspirators are liable in damages to EchoStar.

74. As the developer of a system or technology, and the manufacturer and supplier to a lawful distributor of equipment for the purpose of encrypting a subscription programming signal to enable authorized persons to decode an encrypted subscription programming signal, NagraStar has a civil cause of action against the Digital Store Defendants, and the Co-Conspirators pursuant to section 18(1)(d) of the *Radiocommunication Act* for the loss and damage it has sustained as a result of the Digital Store Defendants', and the Co-Conspirators' activities. Accordingly, the Digital Store Defendants, and the Co-Conspirators are liable in damages to NagraStar.

- 31 -

(ii) **Copyright Infringement**

75. The DISH Software is an original, literary and artistic work in which copyright subsists. NagraStar is the owner of the copyright in the DISH Software, and has licensed same to EchoStar.

76. The Digital Store Defendants' Piracy Technology and services in support thereof (including the IKS servers, "hacked" DISH and ExpressVu Access Cards used in support of the IKS servers, and piracy software components for FTA receivers) are, involve or require a reproduction in whole, or in the alternative, of a substantial part of the DISH Software. Without the consent of the Plaintiffs, the Digital Store Defendants have sold, marketed, offered to the public, distributed, provided, and trafficked in copies of the DISH Software. Accordingly, all copies and articles which were made and based upon or derived from the DISH Software infringe NagraStar's copyright therein and licensing rights thereto held by EchoStar.

77. All copies of the DISH Software and all media and other material forms in which infringing copies of the DISH Software are stored, fixed, expressed or embodied (including all computer disks, tapes and computers) and devices by means of which the Digital Store Defendants' Piracy Technology and services in support thereof were produced (including all computers and computer peripherals) wherever situated are subject to the proprietary claims of the Plaintiffs.

78. The Digital Store Defendants have demonstrated, displayed, by way of trade exposed and offered for sale and hire, marketed and distributed for the purposes of trade the DISH Software. Such actions were taken without the authorization of NagraStar and with the knowledge that this conduct infringed the copyright of NagraStar in the DISH Software and the license rights thereto held by EchoStar.

79. The Plaintiffs did not at any time grant to the Digital Store Defendants any consent or license for the use, production, or reproduction of any of the works comprising the DISH Software.

- 32 -

80. The Digital Store Defendants have also infringed EchoStar's copyright to the specific programming in respect of which EchoStar holds a copyright, by wrongfully facilitating the reception of same by persons who are not EchoStar subscribers, including commercial entities which have furnished performances in public of EchoStar's copyrighted works.

81. Accordingly, the Digital Store Defendants are liable for copyright infringement in the DISH Software and in EchoStar's copyrighted programming.

(iii) Civil Conspiracy

82. Beginning at a time unknown and continuing to the present, the Digital Store Defendants conspired by unlawful means with each other, and with the Co-Conspirators (including suppliers of the Piracy Technology and those to whom they sold Piracy Technology), to deprive EchoStar of revenues, proceeds and profits from the sales of subscriptions and pay-per-view services to which EchoStar was entitled. Particulars of the conspiracy are set out below.

83. The Digital Store Defendants, individually and in concert with the Co-Conspirators, have repeatedly engaged in the following wrongful acts, practices and schemes:

- (a) to assist, aid and abet the illegal and unauthorized reception and decryption of EchoStar's encrypted programming otherwise than in accordance with authorization from the lawful distributor of that signal, contrary to subsection 9(1)(c) of the *Radiocommunication Act*, section 34(2) of the *Interpretation Act*, and section 21 of the *Criminal Code*;
- (b) to distribute, offer for sale, sell, install, modify, operate or possess equipment and devices, or components thereof, without lawful excuse, which are or were intended to be used for a purpose contrary to subsection 9(1)(c) of the *Radiocommunication Act*, being the decoding of EchoStar's encrypted programming otherwise than in

- 33 -

accordance with authorization from the lawful distributor of that signal, contrary to subsection 10(1)(b) of the *Radiocommunication Act*;

- (c) to deprive EchoStar of subscription and pay-per-view revenues and other valuable consideration by trafficking, distributing, and selling the Piracy Technology, and services in support thereof intending to facilitate reception and decryption of EchoStar's encrypted programming otherwise than in accordance with authorization from the lawful distributor of that signal;
- (d) to misappropriate and convert to their own use proprietary rights of EchoStar and their rights to receive revenues therefrom; and
- (e) to interfere with the EchoStar's existing and prospective economic relations by trafficking, distributing and selling the Piracy Technology and services in support thereof to the Co-Conspirators.

84. The identities of the Co-Conspirators are known to the Digital Store Defendants but unknown to EchoStar. The Co-Conspirators agreed to act in concert with the Digital Store Defendants to produce, offer for sale, design, sell, supply, acquire and use Piracy Technology, components thereof, and services in support thereof, which they and the Digital Store Defendants knew or should have known would cause harm and result in losses to EchoStar, by depriving EchoStar of rights, proprietary interests and revenues belonging to them.

85. The particulars of the overt acts engaged in by the Digital Store Defendants and by the Co-Conspirators individually and as members of the conspiracy, are set out above. As a result of the Co-Conspirators' acts in furtherance of the conspiracy, EchoStar has suffered serious and substantial loss, damage and expense, for which the Digital Store Defendants and the Co-Conspirators are liable.

86. Because the Piracy Technology and services in support thereof have only one purpose, namely facilitating the reception and decoding of EchoStar's encrypted programming signals by

- 34 -

persons not entitled to receive them, the damage caused by the acts of the Digital Store Defendants and the Co-Conspirators was knowingly and intentionally directed towards EchoStar, and the Digital Store Defendants and the Co-Conspirators are liable therefor.

**(iv) Conversion**

87. In carrying out their business and undertaking, the Digital Store Defendants and the Co-Conspirators knew or had reason to know that the Piracy Technology, Activations, and services in support thereof:

- (a) are designed, manufactured or produced for the purpose of circumventing EchoStar's encryption, security and billing systems;
- (b) have no commercially significant purpose or use other than to circumvent the Plaintiffs' encryption, security and billing systems; and
- (c) will be used by other persons for the unlawful and unauthorized reception and use of EchoStar's satellite programming signals.

88. EchoStar has a right to receive subscription and pay-per-view revenues, proceeds and profits from DISH Network Programming in the United States and a proprietary interest in this right. In some cases, EchoStar's right to DISH Network Programming is exclusive. By their acts, the Digital Store Defendants and the Co-Conspirators have wrongfully converted and usurped to themselves EchoStar's property, namely the right to subscription and pay-per-view revenues, proceeds and profits, without authority or payment of any kind to EchoStar. EchoStar is therefore entitled to an accounting and disgorgement of all revenues and profits made by the Digital Store Defendants and the Co-Conspirators from the wrongful conversion of EchoStar's property, and damages from the losses of actual and prospective subscription and pay-per-view revenues and proceeds as a result of the Digital Store Defendants' and the Co-Conspirators' acts.

- 35 -

**(v) Unlawful Interference With Economic Relations**

89. By offering, selling, distributing, and trafficking in Piracy Technology and Activations, the Digital Store Defendants and the Co-Conspirators have directly and intentionally facilitated the unauthorized reception and use of DISH Network Programming by persons not authorized to receive it. The Digital Store Defendants and the Co-Conspirators have done these acts in full knowledge of EchoStar's relationships with its subscribers and prospective subscribers, and have knowingly made EchoStar the target of their wrongdoing and caused harm to EchoStar. The Digital Store Defendants and the Co-Conspirators have thereby unlawfully interfered with EchoStar's economic relations with its subscribers and prospective subscribers, and are liable therefor.

90. The Digital Store Defendants and the Co-Conspirators have also unlawfully interfered with EchoStar's economic relations, with knowledge of the same and without lawful excuse, by inducing, procuring, conspiring, aiding and abetting an as yet undetermined number of subscribers to cancel or not renew their contracts with EchoStar and an as yet undetermined number of prospective subscribers to EchoStar to not purchase subscriptions thereby resulting in damage to EchoStar.

91. By reason of the foregoing, the Digital Store Defendants and the Co-Conspirators are liable for all pecuniary losses suffered by EchoStar as a result of their interference.

**(vi) Unjust Enrichment**

92. EchoStar generates its revenues through sales of subscription packages and pay-per-view programming. It is critical to the operations of EchoStar that it be able to make access to DISH Network Programming conditional on the purchase of legitimate subscriptions and pay-per-view programming. For this reason, EchoStar devotes substantial resources to the continued development and improvement of its security system.

93. The sole purpose of the Digital Store Defendants' and the Co-Conspirators' business and undertaking dealing in Piracy Technology and Activations, apart from commercial gain, is to permit

- 36 -

consumers to receive and decode EchoStar's encrypted programming without payment of subscription and pay-per-view fees to EchoStar and thereby receive unlimited DISH Network Programming without charge.

94. The Digital Store Defendants' and the Co-Conspirators' activities have been carried out intentionally, with full knowledge of EchoStar's rights, and without EchoStar's consent. As a direct and proximate result of their wrongful acts, the Digital Store Defendants and the Co-Conspirators have been unjustly enriched and EchoStar has suffered, and will continue to suffer, loss of revenues, proceeds and profits. The exact amount of unjust profits realized by the Digital Store Defendants and the Co-Conspirators and profits lost by EchoStar are presently unknown and cannot be readily ascertained without an accounting.

95. The Digital Store Defendants' and the Co-Conspirators' activities have illegally exploited for commercial gain EchoStar's services and confidential information in its security system. In doing so, they jeopardized the goodwill associated with EchoStar's name and its reputation in the marketplace, which in turn results in continuous losses of revenue, proceeds, profits and other benefits that are impossible to ascertain at this time, and destroy the business relationships and good reputation that EchoStar has developed over many years. It would be unjust to allow the Digital Store Defendants and the Co-Conspirators to retain any of the benefits they have received at EchoStar's expense.

**(vii) Constructive Trust and Equitable Tracing**

96. The Digital Store Defendants received revenues, proceeds, and profits from the illegal activities of the Digital Store Defendants as pleaded herein, with actual or constructive knowledge of the illegality thereof. The Digital Store Defendants used those funds to purchase various assets, property, and interests, including the Wanda Property.

97. Accordingly, the Digital Store Defendants hold their assets, property, and interests, including the Wanda Property, in trust for the benefit of the Plaintiffs and are liable to the Plaintiffs for

- 37 -

repayment of such funds. The Plaintiffs claim a constructive trust over and is entitled to trace the funds into the Digital Store Defendants' assets, property, and interests including the Wanda Property.

98. The Plaintiffs are further entitled to an equitable tracing order to recover all assets, now or previously in the possession of the Digital Store Defendants, acquired directly or indirectly with the Digital Store Defendants' illegal revenues, proceeds and profits.

**(viii) Waiver of Tort**

99. In the alternative to their claim for damages resulting from the wrongful acts of the Digital Store Defendants and the Co-Conspirators, the Plaintiffs plead the doctrine of waiver of tort and waive the torts pleaded herein. The Plaintiffs thus elect to claim payment of the revenues, proceeds, and profits generated by the Digital Store Defendants and the Co-Conspirators as a result of the wrongful acts described above.

**IRREPARABLE HARM**

100. The conduct of the Digital Store Defendants causes, has caused and continues to cause significant and irreparable harm to EchoStar and NagraStar. It deprives EchoStar of subscription and pay-per-view revenues and other valuable consideration. It circumvents the EchoStar Security System, and infringes on trade secrets and confidential and proprietary information, and interferes with EchoStar and NagraStar's contractual and prospective business relations.

101. In particular, the actions of the Digital Store Defendants cause EchoStar and NagraStar irreparable harm in that they:

- (a) deprive EchoStar of an incalculable (as a result of the inability to ascertain, trace or account for all unauthorized uses of DISH Network Programming) number of existing and prospective customers in the United States;
- (b) cause EchoStar a loss of revenues, proceeds, profits and other benefits that is also incalculable, because it is difficult for EchoStar to trace, calculate or prove:

- 38 -

- (i) how many persons are receiving DISH Network Programming without authorization;
  - (ii) how much and which type of DISH Network Programming and how much pay-per-view programming these persons are receiving without authorization; and
  - (iii) the actual value of the DISH Network Programming being received without authorization;
- (c) compromise the integrity of the EchoStar Security System which was developed with the investment of considerable time and expense;
  - (d) exploit for commercial gain EchoStar's and NagraStar's trade secrets and confidential information in the EchoStar Security System;
  - (e) expose EchoStar to claims that it is providing DISH Network Programming to persons in Canada, contrary to the territorial restrictions of its U.S. license and Canadian law;
  - (f) expose EchoStar to claims by persons in Canada who hold rights to the same programming that EchoStar holds the rights to in the U.S. that EchoStar is breaching its copyright restrictions and encroaching on the Canadian market by providing DISH Network Programming in Canada;
  - (g) jeopardize the goodwill associated with EchoStar's name and the reputation in the marketplace, which in turn results in continuous losses of revenue, proceeds, and future business opportunities, profits and other benefits that are impossible to ascertain at this time; and
  - (h) destroy the relationships which EchoStar has developed over many years with its suppliers and customers, including its ability to retain distribution rights for copyrighted programming as a result of its inability to restrict distribution thereof.

102. Because the number of users of the Piracy Technology, software components, keys, and information provided by the Digital Store Defendants is unknown, and the extent and type of programming viewed by these users is highly variable, it is very difficult for EchoStar to calculate the actual losses it sustains, has sustained and continues to sustain as a result of the Digital Store Defendants' actions. Thus, EchoStar has no adequate legal remedy other than the injunctive relief sought in this motion to address the continuing violation of its rights, and bring an end to the Digital Store Defendants' illegal acts.

- 39 -

103. The Piracy Technology and services in support thereof offered by the Digital Store Defendants have facilitated the unauthorized descrambling of EchoStar's scrambled subscription programming signals, without restriction and free of charge, by persons who are not entitled to descramble them. By their activities, the Digital Store Defendants have caused and threaten to cause EchoStar irreparable harm.

#### **DAMAGES**

104. The Plaintiffs sustain an economic loss every time Piracy Technology is used to receive DISH Network Programming and every time Activations are sold for this purpose. As a result of the conduct of the Digital Store Defendants and their Co-Conspirators, the Plaintiffs have suffered damage and expense, while the Digital Store Defendants and the Co-Conspirators have profited from their wrongful activities. The full extent of the Plaintiffs' damages are not known to the Plaintiffs but the Plaintiffs undertake to provide particulars of all such damages prior to the trial of this action.

105. The Digital Store Defendants and their Co-Conspirators have acted in a high-handed, malicious, and reprehensible fashion, and in wanton and reckless disregard for the Plaintiffs' rights, which ought not to be countenanced by this Honourable Court. Accordingly, the Plaintiffs are entitled to punitive, aggravated, and exemplary damages.

106. As a result of the wrongful acts of the Digital Store Defendants and their Co-Conspirators, the Plaintiffs have suffered special damages, particulars of which will be provided prior to trial.

107. The Plaintiffs plead and rely on:

- (a) sections 2, 9(1)(c), 10(1)(b), 18(1)(a) and (d) of the *Radiocommunication Act*, R.S.C. 1985, c. R-2, as amended;
- (b) section 34(2) of the *Interpretation Act*, R.S.C. c. I-23, as amended;

- 40 -

- (c) section 21 of the *Criminal Code*, R.S.C. 1985, c. C-46, as amended; and
- (d) sections 1, 2.4(1), 2.7, 3(1), 5(1), 13(4)(6)(7), 21(1), 27, 34, 34.1, 35, 36, 38.1, and 39.1 of the *Copyright Act*, R.S.C. 1985, c.C-42, as amended.

108. The Plaintiffs propose that this action be tried in Toronto, Ontario.

March 23, 2009

**BORDEN LADNER GERVAIS LLP**  
Scotia Plaza, 40 King Street West  
Toronto, Ontario  
M5H 3Y4

**Christopher D. Bredt**  
LSUC# 23627Q  
Tel: (416) 367-6165  
Fax: (416) 361-7063

**Karen Kiang**  
LSUC# 51322T  
Tel: (416) 367-6202  
Fax: (416) 361-7331

**Lawyers for the Plaintiffs**  
Dish Network LLC, EchoStar Technologies  
LLC, and NagraStar LLC

### SCHEDULE "A" - THE EVIDENCE

- (a) Piracy Technology, including any device, technology, product, service, equipment or apparatus, software, programming code, or any component thereof, which has or may be used, or is or was intended to be used, for the purpose of circumventing the Plaintiffs' security system, thereby permitting or facilitating the unauthorized reception and decoding of EchoStar's encrypted satellite television programming signals ("DISH Network Programming"), and services in support thereof, including, without limiting the generality of the foregoing, free-to-air receivers ("FTA receivers") programmed or modified to facilitate the theft of DISH Network Programming, FTA receivers designed to facilitate the theft of DISH Network Programming through the use of Internet Key Sharing ("IKS") / Control Word Sharing, IKS servers, DISH Access Cards (as defined herein), ExpressVu Access Cards, Internet dongles, piracy software components, and services in support thereof;
- (b) any designs, drawings, diagrams, sketches, schematics, screens, electronic files (including gerber files) or other evidence pertaining to the creation, design, manufacture, or reverse-engineering of Piracy Technology;
- (c) computer equipment and electronic storage media containing any software, programming code, documents, records, graphic files, or electronic data pertaining to the creation, design, manufacture, or reverse-engineering of Piracy Technology or for use with Piracy Technology;
- (d) the Web Sites, the databases contained or stored therein, any data contained therein and the servers on which the Web Sites and Evidence reside;
- (e) any other web site operated by the Digital Defendants containing the Evidence;
- (f) any document, record, note, information, instructions, correspondence sent and received, electronic mail, posts, private messages, and internet relay chat communications (including all such materials fixed on computer disks, CD ROM's, USB drives, flash media, biometric devices, memory cards and sticks, tapes, and any other magnetic or machine readable or electronic storage media) pertaining to:
  - (i) the Digital Defendants' dealings in Piracy Technology or products or services in support thereof or related thereto;
  - (ii) the nature, operation, scale, volume, and extent of the Digital Defendants' business dealing in Piracy Technology, including any and all records of purchase, sale, distribution, or offering of Piracy Technology, including any invoices, financial or accounting records, ledgers, books, accounts, banking records, statements, shipping

documents, source documents, transaction journals, summary reports, financial summaries, web site databases, and online payment processor or auction accounts (including PayPal and eBay);

- (iii) the Digital Defendants' dealings with customers, suppliers, associates, affiliates, users, members, and subscribers, with respect to Piracy Technology and services in support thereof, including the names, addresses, telephone numbers, e-mail addresses, fictional usernames, aliases, Internet Protocol addresses, and other particulars of the identities of any persons who have been provided with or purchased Piracy Technology from or whose business has been solicited by the Digital Defendants for the purpose of selling any Piracy Technology, and including any business cards, datebooks/agendas/diaries, phone records, messages, memoranda, notes, promotional material, literature, brochures and advertising;
- (g) any other evidence of the acts and omissions alleged in the Statement of Claim herein.

Commercial List No.: 09-CL-8091-00CL

- and - RAVINDRANAATH RAMKISSOON, et al.

DISH NETWORK LLC, et al.

**ONTARIO****SUPERIOR COURT OF JUSTICE  
(COMMERCIAL LIST)**

PROCEEDING COMMENCED AT TORONTO

**AMENDED STATEMENT OF CLAIM****BORDEN LADNER GERVAIS LLP**Barristers and Solicitors  
Scotia Plaza  
40 King Street West  
Toronto, Ontario  
M5H 3Y4**Christopher D. Bredt (LSUC# 23627Q)**Tel: (416) 367-6165  
Fax: (416) 361-7063**Karen Kiang (LSUC# 51322T)**Tel: (416) 367-6202  
Fax: (416) 361-7331Lawyers for the Plaintiffs,  
Dish Network LLC, EchoStar Technologies LLC,  
and NagraStar LLC  
::ODMA\FPCDOCS\TOR01\4108241\

## Christine Hagan

---

**From:** Chad Hagan  
**Sent:** Friday, January 22, 2010 2:42 PM  
**To:** Gerald Kelly  
**Cc:** Christine Willetts; Clayton Craighead  
**Subject:** RE: Dish Network, EchoStar Satellite and NagraStar vs Ramkissoon et al

**Importance:** High

Gerald,

Thank you for the call today. As discussed in our email exchange below, your clients were to deliver the subject DISH Network receivers and access cards to your office this week for shipment to NagraStar. You advised during today's call that Munin Ramkissoon claims these receivers, access cards and his laptop computer were "stolen" from his vehicle on the day he was to transport them to your office. As you can imagine, your client's claim is simply not believable. Moreover, it is compounded by his denial of knowing or being related to Ravin Ramkissoon in Canada. We know now that not only is Ravin related to your clients (your clients are his aunt and uncle), but that Ravin visited them in the US shortly after this suit was filed. As previously discussed, Ravin is already embroiled in litigation with NagraStar, DISH Network and BellTV in Canada after an Anton Piller Order was granted and a search and seizure was executed at his residence and business locations.

By your client destroying (or allowing to be destroyed) critical evidence in the case against him in the United States, he has compounded this situation and the problems he will face as this litigation progresses. Please provide us with the address, location and time which he claims his vehicle was broken into and this evidence was "stolen" so that we can immediately initiate efforts to investigate further. Please also caution your clients about any further evidence spoliation and instruct them not to delete, modify, save-over, or otherwise alter any electronically stored information ("ESI") specifically including without limitation all emails stored in their email accounts, and text, pin, sms or any other form of electronic communication engaged in them via phone, computer or other electronic medium.

Our office will begin preparation of the required 26f report, 26a disclosure and a stipulated protective order to be used in the case. I look forward to hearing back from you on the address and time of the alleged "theft" and confirmation that your clients have not tampered with, deleted, destroyed, modified or altered any of their ESI specifically including emails.

Best regards,

Chad M. Hagan  
Hagan Noll & Boyle, LLC  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, Texas 77024  
T: 713.343.0478  
F: 713.758.0146  
chad.hagan@hnbllc.com  
<http://www.hnbllc.com>

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use,

disclosure, dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message and its attachments. To contact us directly, please email [info@hnbllc.com](mailto:info@hnbllc.com). Thank you.

-----Original Message-----

From: Gerald Kelly [<mailto:gjklaw@optonline.net>]  
Sent: Wednesday, January 13, 2010 2:44 PM  
To: Chad Hagan  
Subject: RE: Dish Network, EchoStar Satellite and NagraStar vs Ramkissooon et al

My client will drop off the boxes and access cards next Tuesday. I will call you as soon as I have them.

GERALD J. KELLY, ESQ.  
3125 Rt. 10 East, Suite 2C  
Denville, New Jersey 07834  
Phone: 973-328-1199  
Fax: 973-328-3807  
Cell: 973-945-3554  
Email: [gjklaw@optonline.net](mailto:gjklaw@optonline.net)

-----Original Message-----

From: Chad Hagan [<mailto:chagan@hnbllc.com>]  
Sent: Thursday, January 07, 2010 6:02 PM  
To: Gerald Kelly  
Cc: Christine Willetts  
Subject: RE: Dish Network, EchoStar Satellite and NagraStar vs Ramkissooon et al  
Importance: High

Confidential - subject to FRE 408

Gerald,

Thank you for the call this afternoon. I have discussed with my clients and they have requested as follows:

Please have your clients drop off all 3 of their DISH receivers (with access cards) at your office and we will arrange for a courier service to fedex them to NagraStar's office for analysis. Once that analysis is complete, our client reps can meet with the Ramkissooon's and their son to discuss and to image the computer and laptop. Please ensure proper chain-of-custody why at your office so that no one has access to, or tampers with the receivers or cards. Please DO NOT allow your clients to attempt to mail the receivers directly to NagraStar or your office (I don't want them claiming they were "lost in the mail"). Let us know when they have deposited them at your office and we can arrange for a courier service.

Thanks,

Chad M. Hagan  
Hagan Noll & Boyle, LLC  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, Texas 77024  
T: 713.343.0478  
F: 713.758.0146

chad.hagan@hnbllc.com  
http://www.hnbllc.com

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message and its attachments. To contact us directly, please email [info@hnbllc.com](mailto:info@hnbllc.com). Thank you.

-----Original Message-----

From: Gerald Kelly [mailto:[gjklaw@optonline.net](mailto:gjklaw@optonline.net)]  
Sent: Monday, January 04, 2010 2:55 PM  
To: Chad Hagan  
Subject: RE: Dish Network, EchoStar Satellite and NagraStar vs Ramkissoon et al

I am back in my office now. Please call me on my cell 973-945-3554 so I will pick up if I am in another meeting.

GERALD J. KELLY, ESQ.  
3125 Rt. 10 East, Suite 2C  
Denville, New Jersey 07834  
Phone: 973-328-1199  
Fax: 973-328-3807  
Cell: 973-945-3554  
Email: [gjklaw@optonline.net](mailto:gjklaw@optonline.net)

-----Original Message-----

From: Chad Hagan [mailto:[chagan@hnbllc.com](mailto:chagan@hnbllc.com)]  
Sent: Monday, January 04, 2010 2:04 PM  
To: 'gjklaw@optonline.net'  
Cc: Christine Willetts  
Subject: Re: Dish Network, EchoStar Satellite and NagraStar vs Ramkissoon et al

Gerald,

I just called and left you a voicemail. Let me know when you are available this afternoon to discuss this matter.

Chad M. Hagan  
Hagan Noll & Boyle, LLC  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, Texas 77024  
T: 713.343.0478  
F: 713.758.0146  
[chad.hagan@hnbllc.com](mailto:chad.hagan@hnbllc.com)  
<http://www.hnbllc.com>

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use,

disclosure, dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message and its attachments. To contact us directly, please email [info@hnbllc.com](mailto:info@hnbllc.com). Thank you.

----- Original Message -----

From: Gerald Kelly <[gjklaw@optonline.net](mailto:gjklaw@optonline.net)>

To: Chad Hagan

Sent: Sun Jan 03 12:39:54 2010

Subject: RE: Dish Network, EchoStar Satellite and NagraStar vs Ramkissooon et al

Please call me tomorrow morning. I need to discuss this with you before I file a formal appearance.

GERALD J. KELLY, ESQ.  
3125 Rt. 10 East, Suite 2C  
Denville, New Jersey 07834  
Phone: 973-328-1199  
Fax: 973-328-3807  
Cell: 973-945-3554  
Email: [gjklaw@optonline.net](mailto:gjklaw@optonline.net)

-----Original Message-----

From: Chad Hagan [<mailto:chagan@hnbllc.com>]

Sent: Monday, December 21, 2009 1:31 PM

To: 'gjklaw@optonline.net'

Cc: Christine Willetts

Subject: Dish Network, EchoStar Satellite and NagraStar vs Ramkissooon et al

Mr. Kelly,

Our firm represents DISH Network, EchoStar and NagraStar in the case against the Ramkissooon's. I have been informed by our local counsel that you will be representing the defendants. We need to schedule a call for next week or the following week to discuss the case and set a date for our Rule 26f conference and Rule 26a initial disclosures - as well as a few preservation and electronic discovery matters. Please check your schedule and let me know a date/time when you have availability.

Chad Hagan.

Chad M. Hagan  
Hagan Noll & Boyle, LLC  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, Texas 77024  
T: 713.343.0478  
F: 713.758.0146  
[chad.hagan@hnbllc.com](mailto:chad.hagan@hnbllc.com)  
<http://www.hnbllc.com>

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents or attachments, is strictly prohibited. If you have received this communication in

error, please reply to the sender and destroy all copies of the message and its attachments. To contact us directly, please email [info@hnbllc.com](mailto:info@hnbllc.com). Thank you.

06/09/2010 18:19 973-328-3807

GERALD J KELLY ESQ

PAGE 02/14

GERALD J. KELLY (GK-5646)  
 GERALD J. KELLY, P.C.  
 3125 Route 10 East  
 Denville, New Jersey 07834  
 Telephone: (973) 328-1199  
 Facsimile: (973) 328-3807  
 Attorney for Defendants,  
 Munid Ramkissoon and  
 Ootra Ramkissoon

UNITED STATES DISTRICT COURT  
 FOR THE DISTRICT OF NEW JERSEY

DISH NETWORK L.L.C., A Colorado	:	
Limited Liability Company,	:	Civil Action No.
ECHOSTAR TECHNOLOGIES L.L.C.,	:	2:09-CV-06135-DRD-MAS
A Texas Limited Liability	:	
Company, and NAGRASTAR LLC,	:	
a Colorado Limited Liability	:	
Company	:	
	:	DEFENDANTS' RESPONSE TO
	:	PLAINTIFF'S INTERROGATORIES
Plaintiff,	:	
	:	
vs.	:	
	:	
MUNID RAMKISSOON and OOTRA	:	
RAMKISSOON, and Does 1-10	:	
Defendants	:	

The defendants respond to plaintiff's interrogatories as follows:

ANSWERS TO INTERROGATORIES

1. Munid Ramkissoon, 5 Seasons Glen Drive, Morris Plains, NJ  
 Ootra Ramkissoon, 5 Seasons Glen Drive, Morris plains, NJ  
 Radha Ramkissoon, 235 E. 40<sup>th</sup> Street, Apt. 2H, New York, NY 10016  
 Keshan Ramkissoon, 5 Seasons Glen Drive, Morris Plains, NJ  
 Nandani Ramkissoon, 700 Grove Street, Apt. 10R, Jersey City, NJ 07310
2. It is impossible to give dates and times that each person accessed or used Dish Network equipment since the equipment was located in the home and apparently would be used whenever the television was accessed. The identity and description of the

Dish Network equipment cannot be specified since that equipment was stolen as was previously advised. However, whenever the Dish Network representatives were at the house, they may have taken the serial numbers or identification numbers from the equipment and that would be in the possession of the Dish Network representatives/technicians. The Dish Network equipment was never used or located other than 5 Seasons Glen Drive, Morris Plains, NJ.

3. These defendants have no information with regard to any IKS Servers nor what an IKS Server is.

4. None known to these defendants.

5. These defendants deny engaging in any satellite television piracy and have no knowledge of any Dish Network equipment located in their premises being used by any other person for such uses.

6. These defendants have no information with regard to what an IKS receiver or an FTA receiver is or how it was used and deny any involvement with the use of such technology.

7. These defendants deny any of the above descriptions regarding satellite transmissions, receivers or any of the other information contained in this paragraph.

8. The only information these defendants have are with regard to certain allegations that were made against Ravin Ramkissoon, who resides in Canada. This information was only obtained after representatives of Dish Network contacted these defendants. However, these defendants do not have any information as to the extent of the allegations, any actions that may have been taken by third parties, or whether, in fact, the third parties actually engaged in such activity.

9. Munid Ramkissoon is related to Ravindranauth Ramkissoon (sister's son), Rosaline Ramkissoon (sister's daughter-in-law), Anandanauth Ramkissoon (sister's son). The other named entities have no relationship or interaction with these defendants.

10. Defendants deny any relationship or interaction with any satellite television piracy website.

11. These defendants have no information with regard to anyone allegedly involved in the claims that have been made by the plaintiff in this case.

12. These defendants do not have email addresses and to the best of Munid Ramkissoon's knowledge, he text-messaged one time several months ago. However, he does not utilize text messaging on a regular basis and neither defendant engages in on-line discussion forums, nor any electronic form of communication concerning the persons or entities listed in this question.

13. These defendants do not have any email addresses that are either registered or used by them to exchange electronic communications or any other electronic form of communication relating to any of the individuals or entitles named in this question.

14. On Wednesday, January 20, 2010, defendant, Munid Ramkissoon, had disconnected the equipment, namely, three Dish Network Set-Top Boxes and one HP laptop computer, as well as one GPS unit, in order to deliver the Dish Network Boxes and the computer to the office of Gerald Kelly. Prior to that delivery, Munid Ramkissoon called the attorney's office and the attorney was not in at that time but would be in later in the day. Munid Ramkissoon then traveled to Jersey City for a small contracting job, and while there, his motor vehicle was broken into and the above items were taken. A police report was filed with regard to that incident and is attached.

15. These defendants have no information with regard to any transmission of control words or any other information in this question.

16. The only persons that were contacted concerning the Dish Network Subscription or Dish Network equipment were the representatives of the plaintiff. There were no other persons that were contacted regarding the subscription or equipment.

17. The defendants never connected the Dish Network equipment to any IKS Server.

18. None.

19. The only equipment acquired by these defendants was the one receiver from Dish Network and there were two receivers that were purchased on the street. However, those two receivers were connected by the Dish Network representatives whom the defendants believe retained all of the identification information. These defendants only communicated with other individuals concerning

this lawsuit after being accused by the plaintiffs regarding the Dish Network signals. However, the only persons this was discussed with other than defendants' attorney was defendants' children. Thereafter, Dish Network representatives informed the defendant, Munid Ramkissoon, of some allegations against his nephew Ravine Ramkissoon, and after being informed of that, Munid Ramkissoon contacted Ravine Ramkissoon. At that time, Ravine Ramkissoon denied any involvement in such activity.

20. After being informed that Ravine Ramkissoon had been charged by the plaintiffs with various allegations, defendant Munid Ramkissoon contacted him.

21. Munid Ramkissoon cannot recall the specific date but does recall some representatives of plaintiff coming to his house and questioning about some signal coming out from his house. At that time, he informed them that he had no information about that but that prior to that time, the system had not been working properly in that he had contact Dish Network for them to repair it. Prior to that date, plaintiff's representative said that they would send a new box to the defendant. At the time that these other representatives appeared, Munid Ramkissoon believed that it had something to do with the box being delivered. At this meeting, defendant's son, Keshan, was not present during the whole time but was in the house. The plaintiffs' investigators were inquiring about Ravin Ramkissoon, who Munid Ramkissoon knew as "Boom Boom" and not as Ravin Ramkissoon. The plaintiffs' representatives gave Munid Ramkissoon a card and for him to get back to them with any information that he may have. However, he had already told them that he had no information with regard to what they were talking about and that he had not done anything with regard to these boxes or any signals.

22. After the visit from plaintiffs' investigators on December 8, 2009, Munid Ramkissoon traveled to Canada with his family for a family event and at that time, Munid Ramkissoon spoke with Ravin Ramkissoon about what the investigators were asking of him. It is believed that Munid and Ootra Ramkissoon did not go to Canada until the end of December 2009. That date would have also been after receipt of the Federal Court Complaint. Basically, Munid Ramkissoon just questioned Ravin Ramkissoon what this was all about, since Munid Ramkissoon had no information about any of this and believed that he was only being implicated because of his last name and the fact that a Complaint had been made against Ravin Ramkissoon.

23. The only information received from Ravindranauth Ramkissoon was that the plaintiff had filed a suit against him in Canada and that he had a lawyer and they were going to court to respond to the Complaint.

DATED: June 9, 2010

GERALD J. KELLY, Esq. (GK-5646)  
GERALD J. KELLY, P.C.  
3125 Rt. 10 East, Suite 2C  
Denville, New Jersey 07834  
Telephone: (973) 328-1199  
Facsimile: (973) 328-3807  
Attorney for Defendants, Munid  
Ramkissoon and Ootra Ramkissoon

/s Gerald J. Kelly  
GERALD J. KELLY, ESQ.

AO 88B (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

## UNITED STATES DISTRICT COURT

for the

Eastern District of New York

DISH Network L.L.C. et al.

Plaintiff

v.

Munid Ramkissoon, Ootra Ramkissoon, &amp; Does 1-10

Defendant

Civil Action No. 2:09-cv-06135-DRD-MAS

(If the action is pending in another district, state where:

District of New Jersey )

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS  
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Subpoena Compliance Group, Cablevision Systems Corp. d/b/a Optimum, 1111 Stewart Avenue, Behtpage, NY 11714

☒ **Production:** YOU ARE COMMANDED to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material: See Attachment A

Place: Levy, Ehrlich &amp; Petriello, 60 Park Place, Newark, New Jersey 07102

Date and Time:

08/16/2010 9:00 am

☐ **Inspection of Premises:** YOU ARE COMMANDED to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:

Date and Time:

The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: 07/15/2010

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

Attorney's signature

The name, address, e-mail, and telephone number of the attorney representing (name of party) Plaintiffs

DISH Network L.L.C., EchoStar Technologies L.L.C. &amp; NagraStar LLC, who issues or requests this subpoena, are:

Chad M. Hagan, Hagan Noll &amp; Boyle LLC, 820 Gessner, Suite 940, Houston, Texas 77024, chad.hagan@hnbllc.com, (713) 343-0478

AO 88B (Rev. 06/09) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action (Page 2)

Civil Action No. 2:09-cv-06135-DRD-MAS

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)*

This subpoena for *(name of individual and title, if any)*  
was received by me on *(date)* \_\_\_\_\_.

☐ I served the subpoena by delivering a copy to the named person as follows: \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_; or

☐ I returned the subpoena unexecuted because: \_\_\_\_\_  
\_\_\_\_\_.

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also  
tendered to the witness fees for one day's attendance, and the mileage allowed by law, in the amount of  
\$ \_\_\_\_\_.

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_  
\_\_\_\_\_ *Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

**Federal Rule of Civil Procedure 45 (c), (d), and (e) (Effective 12/1/07)****(c) Protecting a Person Subject to a Subpoena.**

**(1) Avoiding Undue Burden or Expense; Sanctions.** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The issuing court must enforce this duty and impose an appropriate sanction — which may include lost earnings and reasonable attorney's fees — on a party or attorney who fails to comply.

**(2) Command to Produce Materials or Permit Inspection.**

**(A) Appearance Not Required.** A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

**(B) Objections.** A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises — or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the issuing court for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

**(3) Quashing or Modifying a Subpoena.**

**(A) When Required.** On timely motion, the issuing court must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

**(B) When Permitted.** To protect a person subject to or affected by a subpoena, the issuing court may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information;

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party; or

(iii) a person who is neither a party nor a party's officer to incur substantial expense to travel more than 100 miles to attend trial.

**(C) Specifying Conditions as an Alternative.** In the circumstances described in Rule 45(c)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

**(d) Duties in Responding to a Subpoena.**

**(1) Producing Documents or Electronically Stored Information.** These procedures apply to producing documents or electronically stored information:

**(A) Documents.** A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

**(B) Form for Producing Electronically Stored Information Not Specified.** If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

**(C) Electronically Stored Information Produced in Only One Form.** The person responding need not produce the same electronically stored information in more than one form.

**(D) Inaccessible Electronically Stored Information.** The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

**(2) Claiming Privilege or Protection.**

**(A) Information Withheld.** A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

**(B) Information Produced.** If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

**(e) Contempt.** The issuing court may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena. A nonparty's failure to obey must be excused if the subpoena purports to require the nonparty to attend or produce at a place outside the limits of Rule 45(c)(3)(A)(ii).

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

DISH NETWORK L.L.C., a Colorado  
Limited Liability Company, ECHOSTAR  
TECHNOLOGIES L.L.C., a Texas Limited  
Liability Company, and NAGRASTAR LLC,  
a Colorado Limited Liability Company,

Plaintiffs,

v.

MUNID RAMKISSOON, an individual,  
OOTRA RAMKISSOON, an individual, and  
DOES 1-10,

Defendantss.

Civil Action No. 2:09-CV-06135-DRD-MAS

**SUBPOENA ATTACHMENT A**

**SUBPOENA ATTACHMENT "A"**

**DEFINITIONS**

The term "Account" shall be defined as the Optimum subscriber account for the  
telephone number (973) 451-9790.

**REQUESTS**

1. All records and other information relating to the Account or any associated  
accounts including the following:

- a. subscriber names, user names, screen names, or other identities;
- b. mailing addresses, residential addresses, business addresses, email  
addresses, and other contact information;
- c. types of services utilized and length of service (including start and end  
date) for each;

- d. telephone records, including local and long distance telephone connection records, caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);
- e. records of user activity for any email address associated with the Account, including the date, time, length, and method of connections, data transfer volume, user name, and IP addresses;
- f. cable records, including packages and channels subscribed to;
- g. means and source of payment for the Account (including any credit card or bank account numbers) and billing records;
- h. correspondence and other records of contact by any person or entity about the Account, such as "Help Desk" notes; and
- i. any other records or evidence relating to the Account.

DATED: July 15, 2010

**HAGAN NOLL & BOYLE LLC**

By: s/ Chad M. Hagan  
Chad M. Hagan (*pro hac vice*)  
Christine D. Willetts (*pro hac vice*)  
Two Memorial City Plaza  
820 Gessner, Suite 940  
Houston, TX 77024  
Telephone: (713) 343-0478  
Facsimile: (713) 758-0146

**LEVY, EHRLICH & PETRIELLO**  
John Petriello (jjp-6545)  
60 Park Place  
Newark, New Jersey 07102  
Telephone: (973) 854-6700  
Facsimile: (973) 596-1781

**Attorneys for Plaintiffs**



July 20, 2010

*Via First Class Mail*

Chad Hagan, Esq.  
Hagan Noll & Boyle LLC  
820 Gessner, Suite 940  
Houston, Texas 77024

Re: DISH Network L.L.C. et al v. Munid Ramkissooon et al.

Dear Mr. Hagan:

This letter responds to the enclosed subpoena requesting subscriber records from CSC Holdings, LLC ("Cablevision") via a cable television system.

The Cable Communications Policy Act of 1984, § 551(c)(2)(B), prohibits a cable operator from disclosing a subscriber's personally identifiable information, including call detail records, except pursuant to a court order<sup>1</sup> authorizing such disclosure. The Subpoena was not a judicial order. Therefore until Cablevision is served with an order mandating such disclosure, we are prohibited by law from providing you with the information you are requesting. Please note that an acceptable court order must specify the subscriber information that you seek and direct Cablevision to disclose the information pursuant to 47 U.S.C. § 551(c)(2)(B).

Additionally, the Cable Act requires Cablevision to provide the subscriber with advance notice of a court order before producing any records. Accordingly, if you decide to seek an order, the return date for compliance under the order should allow Cablevision at least five (5) additional business days to serve notice to the subscriber.

Please be advised that Cablevision reserves the right to obtain reimbursement of our reasonable costs associated with the production of such records. Further, receipt of your court order does not guarantee retrieval of the information you have requested.


<sup>1</sup> If you are requesting your own call detail records or those of your client, Cablevision can accept a written authorization from the subscriber and a subpoena, in lieu of a court order. The written authorization must expressly direct Cablevision to release the records to his or her representative. Further, the authorization and subpoena must indicate whether you are seeking incoming or outgoing telephone records, or both.

CABLEVISION SYSTEMS CORPORATION  
1111 Stewart Avenue, Bethpage NY 11714-3581  
516 803-2300


Chad Hagan, Esq.  
Hagan Noll & Boyle LLC  
July 20, 2010  
Page 2 of 2

Please contact me at 516-803-3917 if you have any questions regarding this matter.

Sincerely,



John Ma  
Paralegal



Enclosure:

106455

FEB-23-2010 09:21

JUGDES ADMIN RM 170

416 327 5417

P.002/022

CITATION: Dish Network LLC v. Ramkissoo, 2010 ONSC 773  
COURT FILE NO.: 09-8091-00CL  
DATE: 20100223

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:

DISH NETWORK LLC, ECHOSTAR  
TECHNOLOGIES LLC AND  
NAGRASTAR LLC

Plaintiffs

- and -

RAVINDRANAATH RAMKISSOON  
a.k.a RAVIN RAMKISSOON,  
RAVINDRANAUGH RAMKISSOON  
a.k.a. DIGITAL, RAVINDRANAATH  
RAMKISSOON a.k.a.  
THEDIGITALSTORE,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as www.thedigitalstore.com,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as www.nfusionteam.com,  
RAVINDRANAATH RAMKISSOON  
C.O.B. as www.canadasat.com,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as www.dummychat.com,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as www.infusioncanada.com,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as www.infusioncanada.ca,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.nfusiononline.com,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.nfusionrepair.com,  
RAVINDRANAATH RAMKISSOON  
c.o.b. as  
www.nfusionwarrantycenter.com,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.nuvenio.ca,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.infusiondepo.com,  
RAVINDRANAUGH RAMKISSOON

Christopher D. Bredt and  
Denise L. Bamborough, for the Plaintiffs

Brett Moldaver and Brendan Hughes, for the  
Defendants Ravindranauth Ramkissoo and  
Roseline Ramkissoo

FEB-23-2010 09:21

JUGDES ADMIN RM 170

416 327 5417

P.003/022

Page: 2

c.o.b. as DIGITAL R US, ANTHONY  
RAMKISSOON, ROSELINE  
RAMKISSOON, DIGITAL STORE  
INC., E-CANADA SOLUTIONS INC.,  
JOHN DOE, JANE DOE and other  
persons unknown who have conspired  
with the name Defendants

Defendants

AND BETWEEN:

COURT FILE NO:09-8094-00CL

BELL EXPRESSVU LIMITED  
PARTNERSHIP

Plaintiff

RAVINDRANAUTH RAMKISSOON  
a.k.a RAVIN RAMKISSOON,  
RAVINDRANAUGH RAMKISSOON  
a.k.a. DIGITAL, RAVINDRANAUTH  
RAMKISSOON a.k.a.  
THEDIGITALSTORE,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as www.thedigitalstore.com,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as www.nfusionteam.com,  
RAVINDRANAUTH RAMKISSOON  
C.O.B. as www.canadasat.com,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as www.dummychat.com,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as www.infusioncanada.com,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as www.infusioncanada.ca,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.nfusiononline.com,  
RAVINDRANAUGH RAMKISSOON  
c.o.b. as www.nfusionrepair.com,  
RAVINDRANAUTH RAMKISSOON  
c.o.b. as  
www.nfusionwarrantycenter.com,

FEB-23-2010 09:21

JUGDES ADMIN RM 170

416 327 5417

P.004/022

Page: 3

RAVINDRANAUGH RAMKISSOON )  
 c.o.b. as www.nuvenio.ca, )  
 RAVINDRANAUGH RAMKISSOON )  
 c.o.b. as www.infusiondepo.com, )  
 RAVINDRANAUGH RAMKISSOON )  
 c.o.b. as DIGITAL R US, ANTHONY )  
 RAMKISSOON, ROSELINE )  
 RAMKISSOON, DIGITAL STORE )  
 INC., E-CANADA SOLUTIONS INC., )  
 JOHN DOE, JANE DOE and other )  
 persons unknown who have conspired )  
 with the name Defendants )

Defendants )

HEARD: January 21, 22, 28 and 29, 2010

**CUMMING J.****The Motion**

[1] The Plaintiffs in both actions seek an order declaring that the defendants in each action, Ravindranauth Ramkissoon ("Mr. Ramkissoon") and Roseline Ramkissoon ("Ms. Ramkissoon") are in contempt of the *Anton Piller* Orders and Interim Injunctions (referred to as the "Second *Anton Piller* Orders" or simply "Orders") granted by myself on December 14, 2009; see *Dish Network LLC v. Ramkissoon* [2009] O.J. No. 5436 (S.C.J.); *Bell ExpressVu Limited Partnership v. Ramkissoon* [2009] O.J. No. 5434 (S.C.J.). The Plaintiffs allege that Mr. Ramkissoon and Ms. Ramkissoon failed to forthwith disclose, deliver up and grant access to the "Evidence" as defined in s. 1 of the Second *Anton Piller* Orders, including:

- (a) The Acer Laptop;
- (b) The hard drive from the HP Laptop;
- ....
- (d) Hard Drives 1, 2, 5 and 6 to the "IBM Server" or so-called "Old Server"; and
- (e) Another computer referred to as "the second" or "other HP Laptop".

[2] All parties agree that the issues on these contempt motions are identical in both proceedings, that the entirety of the evidence applies to the contempt motions in both proceedings and that the same findings are to be made in respect of the motion in each proceeding.

FEB-23-2010 09:21

JUGDES ADMIN RM 170

416 327 5417

P.005/022

Page: 4

**Background**

[3] The Plaintiffs, Dish Network LLC ("Dish"), Echostar Technologies LLC ("Echostar") and NagraStar LLC ("NagraStar") in action #09-8091-00CL brought an extraordinary *ex parte* motion for *Anton Piller* relief against the defendant Ravindranauth Ramkissoon ("Mr. Ramkissoon"). The requested relief was for a Second *Anton Piller* order on the basis that a previous, First *Anton Piller* Order, detailed below, was frustrated by the actions of Mr. Ramkissoon.

[4] EchoStar is a multi-channel video provider throughout the United States via a Direct Broadcast Satellite ("DBS") system consisting of high-powered satellites with scrambled signals to consumers who have paid a subscription fee. EchoStar operates its DBS system under the trade name "Dish Network". Dish is licensed to broadcast its services in the United States.

[5] NagraStar is a supplier of proprietary technology including a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"), used by EchoStar under licence to scramble its satellite signals.

[6] Bell ExpressVu Limited Partnership ("ExpressVu") is the Plaintiff in the companion action, #09-8094-00CL, and brought a like *ex parte* motion for a Second *Anton Piller* Order in that action with the same allegations as seen in action #09-8091-00CL.

[7] ExpressVu, licensed by the Canadian Radio-Television and Telecommunications Commission ("CRTC"), is the largest provider of direct-to-home satellite-based subscription television programming in Canada. ExpressVu has the exclusive right to authorize the decoding of its satellite signals in Canada (the plaintiffs in the two actions are collectively referred to hereinafter as "the Plaintiffs".)

[8] The Defendant, Mr. Ramkissoon, resides in Ontario and carries on a business known as the "Digital Store" of the Defendant Digital Store Inc., an Ontario corporation, in respect of which he is the directing mind. The Digital Store has business premises at 34 Futurity Gate, Unit #7, Vaughan, Ontario. Mr. Ramkissoon is a computing engineering graduate from a community college. All the evidence indicates he is very knowledgeable about computers, computer technology and the delivery of programming by satellites. The Defendant, Ms. Ramkissoon is the spouse of Mr. Ramkissoon. The Ramkissoons reside at 2901 Jane Street, Suite #91, Toronto.

[9] The Plaintiffs allege in their statements of claim that Mr. Ramkissoon is engaging in so-called satellite piracy, acting through various websites, and directly and indirectly, facilitating the unauthorized reception of Dish and ExpressVu programming by, *inter alia*, selling certain receivers (so-called "nFusion FTA Receivers") and arranging for the release of piracy files and the sale of supportive equipment and devices to enable the receivers to steal Dish and ExpressVu programming for the benefit of unauthorized persons who are not paying customers of EchoStar or ExpressVu.

FEB-23-2010 09:22

JUGDES ADMIN RM 170

416 327 5417 P.006/022

Page: 5

[10] Without a subscription, neither EchoStar nor ExpressVu authorize access to their scrambled programming. Moreover, as EchoStar is not licensed at present by the Government of Canada to permit the descrambling of its scrambled programming signals in Canada, no one has the lawful right to descramble EchoStar's signal in Canada.

**The Background to the Motions for the Second *Anton Piller* Orders**

[11] The Plaintiffs sought orders in March 2009 compelling Mr. Ramkissoo to permit them to forensically copy the drives and files of certain computers in his possession or within his control which they believed contained relevant evidence that Mr. Ramkissoo was likely to conceal, delete or destroy if the orders were not granted.

[12] They submitted that the relief is necessary to preserve evidence of Mr. Ramkissoo's breaches of the *Radiocommunication Act* R.S.C. 1985, c.R-2, as am. and to ensure that the process of this Court is not frustrated prior to the trial of this action.

[13] On March 26, 2009, Lederman J. granted *Anton Piller* Orders and injunctive relief (the "*First Anton Piller Orders*") in the two actions.

[14] The Plaintiffs attempted to execute the *First Anton Piller Orders* on March 30, 2009. They claim they encountered difficulty at the residence of Mr. Ramkissoo, being 2901 Jane Street, Unit 91, Toronto and at the Digital Store at Futurity Gate, Unit 7, Vaughan, Ontario. The evidence indicates that as of March 26, 2009, the Digital Store Web Site was owned, operated and/or promoted by Mr. Ramkissoo.

[15] Mr. Ramkissoo reportedly was at home on March 30, 2009 but would not come to the door despite persistent knocking and he could not be served other than by email, which was done at 11:26 a.m. On March 31, 2009 about 7:30 a.m., the Orders were personally served on Mr. Ramkissoo and explained to him by the Independent Supervising Solicitor ("ISS"). Mr. Ramkissoo was asked to provide his Acer Laptop computer but he did not deliver it until April 1, 2009.

[16] Thousands of files reportedly were deleted from this computer between March 30 and April 1, 2009. The Acer Laptop was imaged about April 2, 2009 pursuant to the *First Anton Piller Orders* and found to contain five fragments of deleted files indicating access to the Dummy Chat Web Site by Superstar on at least five occasions. The fragments indicated that a user named "Superstar" accessed private messages on the Dummy Chat Web Site and that approximately 600 private messages were available.

[17] The affidavit of Mr. Wayne Doney sworn September 14, 2009 at para. 15 sets forth the nature of the very extensive deletions from the Acer Laptop after the Plaintiffs' solicitors knocked unsuccessfully on Mr. Ramkissoo's door with the *First Anton Piller Orders* on March 30, 2009 until the computer was physically obtained pursuant to the Orders April 1, 2009. The actions apparently taken on the computer over that brief time period provide strong evidence that Mr. Ramkissoo is engaged in satellite piracy and the improper decryption of Dish programming and ExpressVu programming.

FEB-23-2010 09:22

JUGDES ADMIN RM 170

416 327 5417

P.007/022

Page: 6

[18] The Dummy Chat Web Site is a piracy forum web site, containing threads related to nFusion-brand FTA receivers and numerous posts made by a user named "Digital" and a user named "Superstar". Evidence suggests that after Mr. Ramkissoon became aware of the court actions and that Digital's posts could be used against the defendants, he deleted Digital's user account and many posts. Only an administrator or moderator of a website is able to delete threads or posts from a forum web site. Superstar is an administrator and moderator on the Dummy Chat Web Site and thus had the ability to delete Digital's user profile and threads.

[19] The Plaintiffs brought contempt motions in September 2009 relating to the First *Anton Piller* Orders in which they allege, *inter alia*, that Mr. Ramkissoon continues to engage in breaches of the *Radiocommunication Act*, by making posts on the web site [www.dummychat.com](http://www.dummychat.com) ("Dummy Chat Web Site") under the username "Superstar". Superstar's posts provide updates regarding the encrypted programming of the Plaintiffs, provide support for decrypting the Plaintiffs' programming, and provide so-called piracy files. The contempt motions in respect of the First *Anton Piller* Orders have yet to be heard by Mr. Justice Lederman.

[20] Between April 1, 2009 (after Mr. Ramkissoon was served with the First *Anton Piller* Orders) and December 7, 2009, Superstar reportedly made more than 1800 posts, including messages providing updates about nFusion FTA Receivers and the Plaintiffs' encrypted programming, technical support for using nFusion FTA Receivers to decode and view the encrypted programming of the Plaintiffs, and piracy files and references to nFusion FTA Receivers and security concerns.

#### **The Granting of the Second *Anton Piller* Orders**

[21] The Plaintiffs' extraordinary motions for the Second *Anton Piller* Orders were granted *ex parte* on December 14, 2009. The primary purpose of the Second *Anton Piller* Orders was to preserve the Evidence located on certain of Mr. Ramkissoon's computers.

[22] In considering the motions, this Court was required to consider whether Second *Anton Piller* Orders should be granted against Mr. Ramkissoon, for the limited purpose of searching for and imaging the computers he uses.

[23] There is evidence that suggests that Mr. Ramkissoon's computers may have been used to access user profiles for Superstar and the users Commickaze and Dummycha on the Dummy Chat Web Site, as set out in paras. 9 to 15 of the Dan Caban affidavit sworn December 9, 2009. These users all have administrative or moderator access to the Dummy Chat Web Site. Additionally, Mr. Ramkissoon has been seen with an HP Laptop computer during November 2009. The data on all of the computers that are the subject of the motions for the Second *Anton Piller* Orders may contain evidence relevant to the Plaintiffs' actions and pending motions for contempt and to vary the First *Anton Piller* Orders.

[24] In my view, and I so found, the Plaintiffs had established a strong *prima facie* case against the Defendants of the likelihood of serious damage, actual or potential, to the Plaintiffs, and very convincing evidence that Mr. Ramkissoon had in his possession incriminating documents or electronic data. In my view, there was a real risk that he might destroy such

FEB-23-2010 09:23

JUGDES ADMIN RM 170

416 327 5417 P.008/022

Page: 7

documents and data before any discovery proceedings could be taken if notice was provided to him in advance of obtaining and serving the Second *Anton Piller* Orders.

[25] An *Anton Piller* order is a pre-trial remedy by which a plaintiff is granted access, without notice, to a defendant's premises to inspect and secure evidence where there is a real concern that this evidence would be removed, destroyed or concealed by the defendant if the defendant were to be given advance notice of the motion for the order.

[26] The jurisdiction to grant *Anton Piller* relief is found in this Court's inherent jurisdiction to ensure that its process is not frustrated or defeated by the destruction or alienation of evidence. There is a strong public interest in ensuring that the court process in civil cases is not frustrated by the suppression of evidence: see generally *Ontario Realty Corp. v. P. Gabriele & Sons Ltd.* (2000), 50 O.R. (3d) 539 at 546-48 (S.C.J.).

[27] The test for granting an *Anton Piller* Order requires a moving party to establish:

- a strong *prima facie* case;
- serious damage, actual or potential, to the plaintiff;
- convincing evidence that the defendant has in its possession incriminating documents or things; and
- that there is a real possibility that the defendant may destroy such material before any court discovery proceedings can be taken.

See *Anton Piller KG v. Manufacturing Process Ltd.*, [1976] 1 All E.R. 779 at 784 (C.A.); *Celanese Canada Inc. v. Murray Demolition Corp.*, 2006 SCC 36 at para. 35.

[28] Lederman J., in granting the First *Anton Piller* Orders, was satisfied that all the requisite criteria were met. He had held that the Plaintiffs had made out a strong *prima facie* case that the Defendants have been engaging in activities that contravene the *Radiocommunications Act* in assisting their customers to pirate the Plaintiffs' programming through selling nFusion FTA Receivers and distributing pirate technology and services in support thereof. Evidence obtained via the First *Anton Piller* Orders or since it was obtained, strongly indicates that Mr. Ramkissoon continues to breach the *Radiocommunication Act* through his posting as Superstar on the Dummy Chat Web Site. Although Mr. Ramkissoon denies that he is Superstar, there are fragments of deleted files to the contrary, as they show that the Superstar user profile has been accessed from Mr. Ramkissoon's personal use Acer Laptop and an IBM Server.

[29] Superstar's postings to the Dummy Chat Web Site advise how to use an nFusion FTA Receiver to decode the Plaintiffs' encrypted programming, broadcast updates regularly and provide piracy files.

FEB-23-2010 09:23

JUGDES ADMIN RM 170

416 327 5417

P.009/022

Page: 8

[30] The Plaintiffs will suffer serious damage should the vital evidence sought through the Second *Anton Piller* Orders not be available as the Plaintiffs may be otherwise unable to prove their case and may continue to suffer serious adverse financial impact through lost sales and loss of competitive position: see *Aldrich et al v. Struk et al.* (1984), 8 C.P.R. (3d) 369 (B.C.S.C.) at 371.

[31] A *prima facie* case established that the Acer Laptop and the IBM Server have been used to login to Superstar's user profile on the Dummy Chat Web Site. The evidence indicates the IBM Desktop has been used to login to the user profiles of Commickaze and Dummycha on the Dummy Chat Web Site. Superstar, Commickaze and Dummycha all have administrator or moderator level access to the Dummy Chat Web Site. The data on the computers sought by the Second *Anton Piller* Orders may contain information relating to satellite piracy.

[32] It is a reasonable *prima facie* inference from the evidence to date that Mr. Ramkissoon is engaged in satellite piracy. The evidence indicates he searched for encryption software and deleted thousands of files on the Acer Laptop as the Plaintiffs were attempting to execute the First *Anton Piller* Orders. It is therefore a reasonable inference that new evidence now existing on his computers will be destroyed or concealed given what happened previously between the time of Mr. Ramkissoon having notice of the First *Anton Piller* Orders and giving up his Acer Laptop for forensic analysis pursuant to that First *Anton Piller* Orders. See *Dunlop Holdings Ltd. & Another v. Staravia*, (1981) D No.1988 at 3 (C.A.), online; LEXIS; *DIRECTTV, Inc. v. Toth et al.*, (26 March 2002), Toronto 02-CV-226455 CM3 (S.C.J.) at para. 8. There is good reason to believe that relevant evidence will be deleted, destroyed or concealed if the administration of justice is left to depend upon the ordinary discovery process. In all, the four elements required to grant an *Anton Piller* order were present.

[33] The Second *Anton Piller* Orders required the delivery up of any and all of the Evidence, wherever situated, and in particular, required Mr. Ramkissoon, anyone acting on his behalf and any person on whom the Orders were served, to disclose the whereabouts of the computers he uses, to facilitate access to them and to render any necessary assistance to the Independent Supervising Solicitor ("ISS") and the persons assisting the ISS to enable the ISS to effectively carry out his/her responsibilities under the Orders.

[34] Although the provisions of the Second *Anton Piller* Orders are expansive in seeking to preserve and secure the requisite Evidence, the provisions also seek to ensure minimal intrusion upon the privacy of, and inconvenience to, Mr. Ramkissoon through compliance with the Orders. The intent is for electronic data contained in the computers to be forensically examined, reproduced and removed into the custody of the ISS, an officer of the Court. Any assertion of solicitor-client privilege in respect of Evidence is protected and such disputed Evidence is not made available to the Plaintiffs except as ordered by the Court.

[35] Although the provisions of the Second *Anton Piller* Orders are lengthy and involve legal language unfamiliar to a layperson, in my view, the provisions are clear and unequivocal. Moreover, the intent is that the ISS will give a straightforward explanation of the provisions of the Orders to the persons upon whom they are served.

FEB-23-2010 09:23

JUGDES ADMIN RM 170

416 327 5417 P.010/022

Page: 9

### **The Execution of the Second *Anton Piller* Orders and the Motions for Findings of Contempt**

[36] Injunctions such as *Anton Piller* orders are “readily enforceable through the court’s contempt power”, and when one party alleges that another has failed to comply with such a court order, a motion for contempt may be made: see Robert J. Sharpe, *Injunctions and Specific Performance*, looseleaf (Aurora: Canada Law Book, 1992) at para. 2.10.

[37] As stated above, *Anton Piller* orders find their legitimacy in the court’s inherent power to prevent the frustration of its process through destruction of evidence. This inherent power extends to finding parties who so frustrate court orders to be in contempt.

[38] A contempt motion is quasi-criminal in nature, as there is a potential for imprisonment. Therefore, proof beyond a reasonable doubt is required.

[39] The plaintiffs are not required to prove that a defendant *intended* to act contemptuously. Instead, the plaintiffs are required to prove that a defendant must have intentionally committed an act prohibited by the Order.

[40] The test for a finding of contempt was considered recently by the Court of Appeal in *Bell ExpressVu Ltd. Partnership v. Torroni*, 2009 ONCA 85, 94 O.R. (3d) 614 [*Torroni*]. In *Torroni*, the court overruled a contempt finding on the basis that the motion judge failed to consider each element in the three-part test for contempt. At para. 21 of the decision, these elements are set forth as follows:

- the order that was breached must state clearly and unequivocally what should and should not be done;
- the party who disobeys the order must do so deliberately and wilfully; and
- the evidence must show contempt beyond a reasonable doubt.

[41] The first prong of the test can be determined by looking at the contents of the Orders. Are they clear? Do they make sense? Are they “clear to a party exactly what must be done to be in compliance with the terms of an order”? *Torroni* at para. 22.

[42] In the second prong of the test, one must consider the conduct of the alleged contemnors. What do their actions demonstrate? Evidence on the conduct of the Ramkissoons included an audio recording, affidavits from the ISS and representatives of legal counsel for the Plaintiffs and *viva voce* evidence from the Ramkissoons themselves.

[43] If there is legitimate confusion about the nature and scope of the contents of the Orders, contempt cannot be made out. In this instance, Orders were issued which allow for a search of the home and business of the Defendants and their cars. The items subject to the Orders are listed at para. 1 of the Orders. The rights and responsibilities of the Ramkissoons are laid out in

FEB-23-2010 09:24

JUGDES ADMIN RM 170

416 327 5417 P.011/022

Page: 10

the Orders, as well as the permissible method of execution. As stated above, the terms are clear and unequivocal.

[44] The rights and responsibilities of the Ramkissoons are clearly spelled out in the Orders, which are to, *inter alia*, allow the ISS to exercise their rights and discharge their duties and require the Defendants to "render any necessary assistance" to the ISS.

[45] Regarding the missing HP hard drive, discussed below, the Defendants complain that the basket clause only includes "computers" in the possession of Mr. Ramkissoon, not "hard drives". However, the Orders state that the computers are required in order to, among other things, reproduce their hard drives and electronic data. Therefore, any reference to a computer necessarily includes the hard drive.

[46] The Defendants point to a single incorrect letter in a serial number in the Orders as proof of ambiguity, which the Plaintiffs attributed to a misreading on their part. In fact, the serial number "78-GXHT6" was written in the Orders as "78-GKHT6." The Orders further qualified that the IBM server in question was Type 8668-27X. In my view, there was not any ambiguity or confusion created by the misstated letter. This conclusion is fortified by the fact that the IBM server was indeed the type it was stated to be in the Orders. Indeed, while not specifically stated in the Orders, the server is the same one which was previously the subject of the First *Anton Piller* Orders.

[47] The case at hand is distinguishable from *Torroni*, where the Court of Appeal found that there was indeed ambiguity and confusion in the terms of the order. In *Torroni*, there were two orders which specified different search areas and there was no list of items subject to the order. Here, there is no such problem.

[48] In my view, and I so find, the Orders are clear and unequivocal as to what should be done and what should not be done by the Defendants. I turn now to the execution of the Orders.

[49] On December 16, 2009, the Plaintiffs' representatives attended at the Digital Store premises at 34 Futurity Gate and the Jane Street residence to execute the Second *Anton Piller* Orders. The representatives included Mark Abradjian ("Abradjian"), Brad Wiseman ("Wiseman") and Renata Kis ("Kis"), the ISS appointed pursuant to the Second *Anton Piller* Orders, Steve Rogers ("Rogers") from the computer forensic firm Digital Evidence International Inc. ("DEI"), and Ira Nishisato ("Nishisato") and Isabella Massimi ("Massimi") from the Plaintiffs' law firm.

[50] Mr. Abradjian, the senior person of the ISS group, was not cross-examined on his affidavit dated December 29, 2009. Nor did counsel for Mr. and Ms. Ramkissoon ask that Mr. Abradjian or Mr. Nishisato be cross-examined at the hearing on the return of the motion for contempt. I accept the affidavit evidence of Mr. Abradjian and Mr. Nishisato and I prefer their evidence where there is conflict with the evidence of Mr. and Ms. Ramkissoon.

[51] I do not find either Mr. Ramkissoon nor Ms. Ramkissoon to be credible witnesses in their testimony, including their recounting of, and explanations for, their actions and behaviour

FEB-23-2010 09:24

JUGDES ADMIN RM 170

416 327 5417 P.012/022

Page: 11

during the execution of the Second *Anton Piller* Orders by the ISS and Plaintiffs' counsel. I accept the evidence of Mr. Abradjian and Mr. Nishisato in preference to that of the Ramkissoons where their evidence is in conflict. I add that the detailed notes of Mr. Abradjian, affixed to his affidavit, as to the events of December 16, 2009, together with the audio recording (and transcription thereof) for part of the time in the course of the events upon the execution of the Orders, support and confirm the affidavit testimony of Messrs. Abradjian and Nishisato and contradict the claims of the Ramkissoons. The audio recording confirms that Messrs. Abradjian and Nishisato calmly and patiently tried to explain why they were on the premises, the efforts at service of the Second *Anton Piller* Orders, the efforts at explaining the contents and nature of the Orders, and that they were seeking to preserve and protect the Evidence.

[52] Mr. Abradjian states that the execution of the Second *Anton Piller* Orders commenced at about 5:23 p.m. December 16, 2009 when Mr. and Ms. Ramkissoon arrived by car outside the Digital Store. Mr. Ramkissoon entered the Digital Store. Ms. Ramkissoon waited in the car. The Digital Store has a carpeted store area with a doorway leading to a hallway and outer office area with a back office which is entered by a doorway from the outer office area.

[53] Mr. Abradjian, followed by Mr. Nishisato within about 30 seconds, entered the premises following upon Mr. Ramkissoon's entrance. Mr. Abradjian states that Mr. Ramkissoon and another man, later determined to be Mr. Krishna Ramkissoon ("Krishna"), met him just inside the doorway leading from the carpeted store area into the outer office area. Mr. Abradjian says he identified himself as the ISS appointed officer pursuant to a Court Order and observed Mr. Nishisato identify himself and attempt to serve the Orders on both of them, together with a box containing the court materials to be served, although the Orders were not taken by Mr. Ramkissoon.

[54] Mr. Abradjian says he explained that the Second *Anton Piller* Orders required them to permit entry to the premises and that he wished to explain the Orders. Mr. Ramkissoon said he wanted to call his lawyer and took out his cell phone whereupon Mr. Abradjian says he said that Mr. Ramkissoon would have an opportunity to call his lawyer but was asked to put down his cell phone until Mr. Abradjian had a chance to explain the Orders and that nothing would happen while he explained it.

[55] Mr. Abradjian states that he was "...trying to ease a tense situation and was continuing to try to explain that they would have an opportunity to refuse entry to certain people for up to two hours and speak to their lawyers and that we could all go into the store area where I could explain the Order in an orderly way....".

[56] Mr. Nishisato confirms the account by Mr. Abradjian in Mr. Nishisato's own affidavit. Mr. Nishisato says he attempted to serve the Orders but that Mr. Ramkissoon refused to accept them. Mr. Nishisato says that Mr. Ramkissoon:

refused to permit Abradjian to explain the Orders at this time and walked back towards the Office, and out of our view, with his phone to his ear....Krishna emerged from the Outer Office Area into the Hallway where Abradjian and I were

FEB-23-2010 09:26

JUGDES ADMIN RM 170

416 327 5417

P.013/022

Page: 12

standing ...[and] would not permit Abradjian to move towards the Office to observe Ravin and physically blocked Abradjian's way.

[57] Ms. Ramkissoon had entered the premises by this point and was served by Mr. Nishisato. Mr. Abradjian states that Ms. Ramkissoon "took up the cause of demanding we leave and was insisting that we leave into the front store area and was edging us out of the back area".

[58] Ms. Ramkissoon prevented the passage of Messrs. Abradjian and Nishisato beyond the doorway from the store area into the outer office area while Mr. Ramkissoon went to the back office where he called his lawyer but could not be seen.

[59] Mr. Abradjian says that he then called counsel for the Ramkissoons, and explained that he had the *ex parte* Second Anton Piller Orders and that he, Mr. Abradjian, had an obligation:

to make sure that evidence was protected and I asked that they advise everyone to come into the front area so that we could explain the Order and proceed in an orderly manner.

[60] Mr. Moldaver, counsel for the Defendants, reportedly asked Mr. Abradjian to allow him to speak with Mr. Nishisato and Mr. Abradjian states that:

I said he could but that I would prefer if everyone come out into the front area. I explained to him that evidence may be deleted in the back. He asked why I had that concern. I said I was concerned because I could not see Mr. Ramkissoon and I was concerned there may be computers back there and they may be deleting or destroying evidence.

[61] The phone records establish that Mr. Ramkissoon spoke with his counsel for 10 minutes from 5:27 p.m. to 5:37 p.m. Mr. Nishisato's affidavit also states that the Orders were served upon the Ramkissoons' counsel by email about 5:37 p.m. and that copies were delivered personally to Mr. Moldaver at approximately 6:10 p.m.

[62] Following upon further discussions between counsel, Mr. Moldaver and Mr. Nishisato agreed on a process to facilitate the execution of the Orders. Mr. Abradjian then explained the Orders to the Ramkissoons and, at approximately 7:55 p.m., the implementation of the search began with the ISS, Nishisato and Rogers, a computer forensic expert from DEI, walking through the premises to identify the Evidence.

[63] Mr. Abradjian states that, for the better part of the first hour following his initial entry, the Ramkissoons and Krishna "refused to allow me into the back office area and refused to come out the front store area for an explanation of the Order...":

I explained to both Mr. Ramkissoon and Mrs. Ramkissoon that I was concerned with the possibility that evidence could be deleted while Mr. Ramkissoon was in the back and Mrs. Ramkissoon refused entry thereto and my requests to attend in the backroom were repeatedly refused.

FEB-23-2010 09:25

JUGDES ADMIN RM 170

416 327 5417 P.014/022

Page: 13

[64] While it is understandable that the Ramkissoons would be surprised and angry about the fact of the Orders, they knew the purpose of those Orders and the importance of being cooperative. They had experienced the execution of the First *Anton Piller* Orders and their aftermath. The Ramkissoons knew the Plaintiffs' accusations that they had deliberately prevented timely access to the execution of the First *Anton Piller* Orders. They were aware of the Plaintiffs' accusations that Mr. Ramkissoon had deliberately destroyed evidence while delaying access.

[65] Moreover, the Ramkissoons knew there was no objection to their calling their counsel, with privacy, for advice. Indeed, Mr. Nishisato told them he wanted them to speak with their counsel. But they also knew that the ISS wanted to keep Mr. Ramkissoon away from the Evidence while the ISS explained the nature of the Orders and while counsel was being contacted. The Ramkissoons knew that the predominant concern of the ISS and Plaintiffs' counsel from the point of their entry to the premises was to ensure that the Evidence was preserved and protected. The Ramkissoons knew and understood that Messrs. Abradjian and Nishisato had real and serious concerns that the Orders might be compromised and rendered ineffective if they could not ensure that the premises and Evidence therein were secure while they explained the Orders and the Ramkissoons spoke with their counsel. Indeed, from 5:27 p.m. to 5:37 p.m., Mr. Ramkissoon spoke with his counsel but Mr. and Ms. Ramkissoon denied the ISS and Mr. Nishisato access beyond the doorway of the store area into the outer office area and the back office until about 6:55 p.m.

[66] Diagrams or sketches of the premises were put into evidence by both sides to the dispute. I find on the evidence that Mr. Ramkissoon and Krishna could not be observed by the ISS and Mr. Nishisato for much of the time between 5:23 p.m. and 6:55 p.m. such that the objective of preserving the Evidence was compromised and jeopardized by their actions and the actions of Ms. Ramkissoon.

[67] Computers that are the subject of the Second *Anton Piller* Orders were determined to be in the outer office area and the back office beyond the view of the ISS and Mr. Nishisato but were not delivered up to the ISS prior to 7:55 p.m.

[68] Mr. Ramkissoon and Ms. Ramkissoon refused to permit the ISS to fully explain the Second *Anton Piller* Orders between 5:20 p.m. and 6:55 p.m. despite repeated requests by the ISS to be able to do so. Telephone discussions between Messrs. Nishisato and Abradjian with Mr. Moldaver ultimately resulted in the ISS gaining access about 7:55 p.m. to the outer office area and the back office for the purpose of effectively executing the Second *Anton Piller* Orders.

[69] I find beyond any reasonable doubt on the evidence that Mr. and Ms. Ramkissoon intentionally did not disclose, deliver up and grant access to the outer office area and back office in a timely manner during the execution of the Second *Anton Piller* Orders. They wilfully and deliberately blocked and prevented entry and access to these areas of the premises to frustrate the purpose of the Orders in preserving the Evidence. They intentionally prevented the ISS upon their entry to the premises from being able to observe Mr. Ramkissoon and Krishna who had access to the Evidence in the outer office area and back office. They were intentionally in breach of ss. 2, 4, 5, 17, 18 and 19 of the Orders by not allowing the ISS to keep the Evidence under

FEB-23-2010 09:25

JUGDES ADMIN RM 170

416 327 5417 P.015/022

Page: 14

observation until access would be granted. They did not render the necessary assistance to the ISS to effectively carry out their responsibilities under the Orders.

[70] I find beyond a reasonable doubt that the Ramkissoons deliberately and wilfully disobeyed the Second *Anton Piller* Orders. I find that Mr. and Ms. Ramkissoon are in contempt of the Second *Anton Piller* Orders. I turn now to a consideration of the specific components of the Evidence sought through the Second *Anton Piller* Orders.

#### **The Acer Laptop**

[71] To date, the Acer Laptop has not been disclosed or delivered up to the ISS. I find with respect to the Acer Laptop that the evidence of Mr. Ramkissoon and Ms. Ramkissoon as to giving it to their seven year old daughter, who then lost it, is not credible.

[72] In response to a query as to the whereabouts of the Acer Laptop, (paragraphs 1(a) and 17 of the Second *Anton Piller* Orders), Mr. Ramkissoon said it was "lost a long time ago". In his affidavit sworn January 8, 2010 in response to the contempt motion, Mr. Ramkissoon states he gave the Acer Laptop to his seven year old daughter in July, 2009 and that she had lost it about a month before swearing his affidavit. Mr. Ramkissoon says his daughter used the Acer Laptop primarily to access the internet, but Ms. Ramkissoon states her daughter was not allowed to conduct searches of the internet. Ms. Ramkissoon said that a replacement Toshiba laptop was purchased in New Jersey whereas Mr. Ramkissoon says it was purchased in Toronto. Ms. Ramkissoon said that their daughter still had the Toshiba laptop, given to her at Christmas, but Mr. Ramkissoon said that it was then exchanged for an HP Laptop after Christmas.

[73] I find the evidence of Mr. and Ms. Ramkissoon in respect of the whereabouts and fate of the Acer Laptop to be implausible. They strike me as parties prepared to say anything at all in an attempt to extricate themselves from the situation they are in. I do not believe them.

[74] However, there is no evidence presented by the Plaintiffs that Mr. Ramkissoon has used the Acer Laptop since it was returned to him following upon the execution of the First *Anton Piller* Orders.

[75] I find that the Plaintiffs have not established beyond a reasonable doubt that Mr. Ramkissoon still has the Acer Laptop. There is not sufficient evidence to support the accusation that he deliberately and wilfully disobeyed the Second *Anton Piller* Orders in respect of the Acer Laptop. Accordingly, in respect of this component of the Evidence, there cannot be any finding of contempt.

#### **The HP Laptop**

[76] Paragraphs 1(b) and 17 of the Second *Anton Piller* Orders require Mr. Ramkissoon to forthwith disclose, deliver up and grant access to the HP Laptop. Mr. Ramkissoon states in his affidavit that he uses the HP Laptop "constantly" and it is his only laptop. The evidence indicates he uses it some eight hours a day. In previous affidavits dated October 14, 2009 and November 17, 2009 in this action, Mr. Ramkissoon has also stated that the information contained on his laptop computer is very valuable and would be of value to his competitors.

FEB-23-2010 09:26

JUGDES ADMIN RM 170

416 327 5417

P.016/022

Page: 15

[77] Mr. Ramkissoon told the ISS during the execution of the Second *Anton Piller* Orders that he would give the ISS the HP Laptop which was shown to be on a desk in his back office but a few minutes later told them that the HP Laptop had no hard drive in it. I find, with respect to the missing hard drive in respect of the HP Laptop, that Mr. Ramkissoon's evidence is not credible.

[78] Mr. Rogers determined that there was no hard drive in the HP Laptop and that two screws used to secure the panel for the hard drive had been damaged and it appeared they had been removed and put back in. Mr. Ramkissoon did not give any explanation to Messrs. Abradjian and Nishisato as to why the hard drive was missing or its whereabouts. He did refer to a "Best Buy" sticker on the underside of the HP Laptop and stated that the HP Laptop was no longer under warranty and Best Buy had refused to service it because he had installed a different operating system on it which voided the warranty. Asked as to whether the hard drive was at Best Buy, he said it was not and did not provide any other explanation as to why the hard drive was missing or where it was.

[79] There was undisputed testimony that the hard drive in question would be some 4 inches by 2 inches by ½ inch thick. Ms. Ramkissoon was asked by Mr. Abradjian if she would allow a search of her purse to determine if the missing hard drive was there. However, she telephoned Mr. Moldaver and on his advice she refused to permit a search of her purse. Ms. Ramkissoon acknowledges on her cross-examination that she understood the reason for the request to search her purse. Moreover, she admits she had an opportunity to meet with Mr. Ramkissoon outside of the observation of the ISS. Moreover, Krishna had met with Mr. Ramkissoon outside the presence of the ISS and left the Digital Store about 10:00 p.m.

[80] Mr. Ramkissoon now states in his affidavit dated January 8, 2010 (at paragraphs 21 and 22) that the HP Laptop stopped working about December 14, 2009 (in his cross-examination he says December 13, 2009) while he was on holidays in New Jersey in the United States. He says he sought to have it replaced December 14, 2009 at the Best Buy store in New Jersey where he had previously purchased it. He says Best Buy told him that the hard drive would not be replaced because of changes to the operating system which voided the warranty. He says he threw away the non-functioning hard drive that day while at the Best Buy store. He returned to Toronto December 15, 2009. He says he had the HP Laptop, minus any hard drive, in his backpack when he entered the Digital Store on December 16, 2010 and took the HP Laptop out of his backpack even though he had not planned to stay long.

[81] There is common ground that at the time of the execution of the Orders on December 16, 2009, a "Best Buy" sticker with the date of December 14, 2009, was affixed to the HP Laptop. This sticker suggests, at the least, that Mr. Ramkissoon was in a Best Buy store with the HP Laptop on December 14, 2009.

[82] Mr. Rogers, a forensic computer expert, states in an affidavit of January 11, 2010 that, in his experience, where there is the installation of a new operating system the warranty will still cover the cost of repairing or replacing defective hardware components, including the hard drive. Moreover, the evidence establishes that the Best Buy warranty is only an extended warranty and,

FEB-23-2010 09:26

JUGDES ADMIN RM 170

416 327 5417 P.017/022

Page: 16

even if it is not honoured, there is an underlying manufacturer's warranty which may still have force.

[83] It is implausible and counterintuitive that Mr. Ramkissoon would throw away a hard drive without first ensuring that the data (which is very important in Mr. Ramkissoon's opinion) stored on it could not be recovered and transferred to another device. Mr. Rogers states that data stored on a hard drive may still be recovered even if the software loaded on the hard drive has stopped functioning. (Mr. Ramkissoon was not questioned as to having 'back-up' through an external hard drive.)

[84] It is also implausible that Mr. Ramkissoon would simply throw away a hard drive in a public place given that there is a risk that the data and confidential information stored on the hard drive might be obtained and accessed by others. It is implausible that he would not purchase a new hard drive immediately if he had indeed discarded the hard drive December 14.

[85] It is implausible that Mr. Ramkissoon would take his HP Laptop with him, in a knapsack, to the Digital Store on December 16, 2009 without a hard drive and implausible he would take out of the knapsack the purportedly inoperative HP Laptop and place it on a desk, especially when he was supposedly only stopping briefly at the Digital Store and his wife was waiting for him in their car outside.

[86] Finally, it is simply very implausible that if Mr. Ramkissoon, a man who lives with his computer and uses his computer for business and personal matters all day long, would go from December 13 to December 17, 2009 without a hard drive for his HP Laptop. He has produced evidence that he purchased a hard drive on December 17, 2009 in Toronto but that is simply self-serving evidence to rationalize his explanation as to why there was no hard drive at the point in time of the execution of the Second *Anton Piller* Orders on December 16, 2009.

[87] As I have said, I do not find Mr. Ramkissoon to be a credible witness. An example of his lack of credibility is seen in his answer to questions relating to his trip to New Jersey to visit his aunt and uncle, Mumid Ramkissoon and Ootra Ramkissoon, in December 2009. Dish, EchoStar and NagraStar had started a lawsuit in New Jersey on December 4, 2009 against the aunt and uncle, alleging that Dish Network technology was being used by them for purposes of satellite piracy. A representative of EchoStar had visited the aunt and uncle to discuss the lawsuit on December 8, 2009. The Defendants, Mr. and Ms. Ramkissoon, arrived in New Jersey December 10 or 11, 2009 but Mr. Ramkissoon denied on cross-examination that he had had any discussions with his uncle and aunt about the lawsuit against them during the visit. This answer of Mr. Ramkissoon is simply implausible, especially considering that the subject matter of the lawsuit against the aunt and uncle is the same as the court actions at hand in which the Ramkissoons are involved. Ms. Ramkissoon also denied that there were any discussions with the aunt and uncle about the lawsuit or that the purpose of their last-minute trip to New Jersey had anything to do with the fact that the aunt and uncle were being sued.

[88] I find that the Best Buy sticker on the back of the HP Laptop on December 16, 2009 evidences only the fact that Mr. Ramkissoon was in a Best Buy store December 14 with his computer and may have purchased some service or part.

FEB-23-2010 09:27

JUGDES ADMIN RM 170

416 327 5417

P.018/022

Page: 17

[89] Considering the totality of the evidence, I make the reasonable inference that the hard drive for the HP Laptop was situated in the HP Laptop at the time of the attempted execution of the Second *Anton Piller* Orders but was removed by Mr. Ramkissoo and hidden by him during the time he could not be seen by Messrs. Abradjian and Nishisato while they were being blocked and frustrated in trying to get access to, and observation of, the Evidence in the back office. Considering the totality of the evidence, I find that it has been proven beyond a reasonable doubt that Mr. Ramkissoo deliberately and wilfully disobeyed the Second *Anton Piller* Orders, and in particular, ss. 1 (b) and 17 thereof in removing the hard drive from the HP Laptop so that the ISS would not gain possession for the purpose of imaging the hard drive and making a copy of the information thereon for the purpose of preserving possible relevant evidence in the actions. I find he is in contempt for not delivering up to the ISS the HP Laptop together with its hard drive.

#### The Old Server

[90] Mr. Ramkissoo and Ms. Ramkissoo state in their responding affidavits that the Old Server was not used since the time of execution of the Second *Anton Piller* Orders.

[91] Sections 1(d) and 17 of the Second *Anton Piller* Orders require Mr. Ramkissoo to disclose, deliver up and grant access to the Old Server. The unique serial numbers for the six hard drives on the Old Server had been noted by DEI at the time of the execution of the First *Anton Piller* Orders. At that time the Old Server had been functioning as a server. The six hard drives contained within the Old Server, as determined pursuant to the execution of the First *Anton Piller* Orders, were configured in such a way that the data was dispersed across all of the hard drives in an "array" and each of the six hard drives was "marked" as part of the array. This is typical for hard drives that make up part of a server and generally, hard drives that are part of a server are part of the same array.

[92] The Old Server was sitting on a desk, with six hard drives inside, in the outer office area during the execution of the Second *Anton Piller* Orders. However, I find on the evidence that the Old Server could not be seen by Mr. Nishisato or Mr. Abradjian when they were standing in the showroom doorway and were prevented by Ms. Ramkissoo and Krishna from following Mr. Ramkissoo and keeping him within their line of vision. Mr. Ramkissoo had a period of time of unsupervised access to the Old Server while Mr. Nishisato and the ISS were prevented from executing the Second *Anton Piller* Orders.

[93] Mr. Rogers states that, during the execution of the Second *Anton Piller* Orders on December 16, 2009, Mr. Ramkissoo objected to Mr. Rogers examining the serial numbers of the four loose hard drives sitting on top of the Old Server. Mr. Ramkissoo also refused to allow the four loose hard drives to be taken into the custody of the ISS and to be copied. There is no plausible good reason for Mr. Ramkissoo making these objections.

[94] Mr. Rogers determined the next day, December 17, 2009, that the serial numbers of the four loose hard drives he had seen sitting on top of the Old Server (and which he had noted) on December 16, 2009 were identical to four of the six hard drives (hard drives 1, 2, 5 and 6) contained in the Old Server during the execution of the First *Anton Piller* Orders. The DEI determined through their examination of the Old Server on December 17, 2009 at the ISS' office

FEB-23-2010 09:27

JUGDES ADMIN RM 170

416 327 5417 P.019/022

Page: 18

that hard drives 3 and 4 (as identified at the time of the execution of the First *Anton Piller* Orders in March/April, 2009) were configured in a way that would be consistent with their forming part of an "array" within the Old Server, together with hard drives 1, 2, 5 and 6 (such as to reasonably lead to the inference that all six hard drives are meant to be connected together for functioning purposes).

[95] The four remaining hard drives found in the Old Server on December 16, 2009 (*i.e.* other than hard drives 3 and 4 as previously identified at the time of execution of the First *Anton Piller* Orders) at the time of execution of the Second *Anton Piller* Orders were determined by Mr. Rogers to not be configured as part of an "array", and to apparently not contain any data. Thus, the format and configuration of the four "new" hard drives (found December 16, 2009, within the Old Server), together with hard drives 3 and 4 in the Old Server, is such that they would not be capable of functioning in any manner, including as a server.

[96] It is a reasonable inference that hard drives 1, 2, 5 and 6 were removed by Mr. Ramkissoon, or at his direction, from the Old Server and were placed on top of the Old Server at some point after the entry of Messrs. Abradjian and Nishisato to the premises but before the time the ISS and DEI were permitted to identify the Evidence during the execution of the Second *Anton Piller* Orders. The reasonable inference is that new hard drives were simply inserted into the trays in replacement of the original hard drives 1, 2, 5 and 6. Such replacement could be done quickly and easily without the need of any tools and without the need of fastening or other manipulation. I would add that the evidence establishes that Mr. Ramkissoon certainly would know that the four loose hard drives (*i.e.* hard drives 1, 2, 5 and 6) on top of the Old Server on December 16, 2009 were necessary for a functioning Old Server given that they were part of the array configuration.

[97] Mr. Ramkissoon asserts that the four loose hard drives found on top of (and not inside of) the Old Server, were not properly part of the Evidence as defined by the Second *Anton Piller* Orders. I find that the loose hard drives were intentionally removed by Mr. Ramkissoon, placed on top of the Old Server, and replacement hard drives were inserted into the server so as to render the server useless in providing evidence, in contravention of his obligations under the Second *Anton Piller* Orders.

[98] Moreover, I add that, in my view, the description in the Second *Anton Piller* Orders in respect of the Old Server means a functioning Old Server. Given the array configuration (as known to Mr. Ramkissoon), the Old Server was not a functioning server without the proper hard drives to make up the array configuration. Mr. Ramkissoon was under an obligation to be cooperative and deliver up the Evidence stipulated by the Second *Anton Piller* Orders. This obliged him to deliver up the four loose hard drives. Although they were ultimately voluntarily delivered up for copying by the DEI (pursuant to the demand of the Plaintiffs' counsel) just before the hearing of the contempt motions, this does not change the fact that Mr. Ramkissoon was in contempt for his deliberate and wilful failure to meet his obligations under the Second *Anton Piller* Orders on December 16, 2009. It is quite possible that the DEI will be unable to determine whether those four hard drives have the same information as they did on December 16, 2009 when the Second *Anton Piller* Orders were executed.

FEB-23-2010 09:28

JUGDES ADMIN RM 170

416 327 5417

P.020/022

Page: 19

[99] I find that it has been proven beyond a reasonable doubt that Mr. Ramkissoon deliberately and wilfully disobeyed the Second *Anton Piller* Orders, and in particular, ss. 1 (d) and 17 thereof in removing hard drives 1, 2, 5 and 6 from the HP Laptop so that the ISS would not gain possession for the purpose of imaging these hard drives and making a copy of the information thereon through the array configuration for the purpose of preserving possible relevant evidence in the actions. I find that Mr. Ramkissoon is in contempt of the Second *Anton Piller* Orders by reason of his deliberate and wilful failure to deliver up the four loose hard drives situated on top of the Old Server, and for his refusal to allow the ISS to remove those loose hard drives, at the time of the execution of the Second *Anton Piller* Orders on December 16, 2009.

#### **The Second or Other HP Laptop**

[100] During the execution of the Second *Anton Piller* Orders, Mr. Nishisato stated that he observed that the HP Laptop (without the hard drive) located in the back office of Mr. Ramkissoon on December 16, 2009 was not the same as an HP laptop seen in use by Mr. Ramkissoon at the Rule 39.03 examination of his uncle, Vijay Ramkissoon, November 25, 2009. Mr. Ramkissoon responded to Mr. Nishisato's query, in the presence of the ISS, that the HP Laptop located in his office December 16, 2009 is the only HP laptop he has, and that there is no HP laptop of his at his residence.


[101] The Defendants do not question the credibility of Mr. Nishisato. In my view, there is a reasonable chance that Mr. Nishisato may be honestly mistaken on this point. I find there is insufficient evidence beyond a reasonable doubt to make a finding of contempt on this asserted item of the Evidence.

#### **Disposition**

[102] For the reasons given, I find that Mr. Ramkissoon and Ms. Ramkissoon are in contempt of the Second *Anton Piller* Orders.

[103] The Second *Anton Piller* Orders remain in force. Mr. Ramkissoon is ordered to purge forthwith his continuing contempt by disclosing, delivering up and granting access to the hard drive for the HP Laptop.

[104] An order will issue in accordance with these reasons and findings. A date for the sentencing hearing will be fixed after consultation with counsel. Any submissions as to costs may be made at the time of the sentencing hearing.

  
CUMMING J.

Released: February 23, 2010

FEB-23-2010 09:28

JUGDES ADMIN RM 170

416 327 5417

P.021/022

CITATION: Dish Network LLC v. Ramkissoon, 2010 ONSC 773

COURT FILE NO.: 09-8091-00CL

ONTARIO

SUPERIOR COURT OF JUSTICE

BETWEEN:

---

DISH NETWORK LLC, ECHOSTAR  
TECHNOLOGIES LLC AND NAGRASTAR LLC

Plaintiffs

-- and --

RAVINDRANAATH RAMKISSOON a.k.a RAVIN  
RAMKISSOON, RAVINDRANAUGH  
RAMKISSOON a.k.a. DIGITAL,  
RAVINDRANAATH RAMKISSOON a.k.a.  
THEDIGITALSTORE, RAVINDRANAATH  
RAMKISSOON c.o.b. as www.thedigitalstore.com,  
RAVINDRANAATH RAMKISSOON c.o.b. as  
www.nfusionteam.com, RAVINDRANAATH  
RAMKISSOON C.O.B. as www.canadasat.com,  
RAVINDRANAATH RAMKISSOON c.o.b. as  
www.dummychat.com, RAVINDRANAATH  
RAMKISSOON c.o.b. as www.infusioncanada.com,  
RAVINDRANAATH RAMKISSOON c.o.b. as  
www.infusioncanada.ca, RAVINDRANAUGH  
RAMKISSOON c.o.b. as www.nfusiononline.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
www.nfusionrepair.com, RAVINDRANAATH  
RAMKISSOON c.o.b. as  
www.nfusionwarrantycenter.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
www.nuvenio.ca, RAVINDRANAUGH  
RAMKISSOON c.o.b. as www.infusiondepo.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
DIGITAL R US, ANTHONY RAMKISSOON,  
ROSELINE RAMKISSOON, DIGITAL STORE

---

FEB-23-2010 09:28

JUGDES ADMIN RM 170

416 327 5417

P.022/022

Page: 2

INC., E-CANADA SOLUTIONS INC., JOHN DOE,  
JANE DOE and other persons unknown who have  
conspired with the name Defendants

Defendants

AND BETWEEN:

COURT FILE NO:09-8094-00CL

BELL EXPRESSVU LIMITED PARTNERSHIP

Plaintiff

RAVINDRANAUTH RAMKISSOON a.k.a RAVIN  
RAMKISSOON, RAVINDRANAUGH  
RAMKISSOON a.k.a. DIGITAL,  
RAVINDRANAUTH RAMKISSOON a.k.a.  
THEDIGITALSTORE, RAVINDRANAUTH  
RAMKISSOON c.o.b. as www.thedigitalstore.com,  
RAVINDRANAUTH RAMKISSOON c.o.b. as  
www.nfusioncam.com, RAVINDRANAUTH  
RAMKISSOON C.O.B. as www.canadasat.com,  
RAVINDRANAUTH RAMKISSOON c.o.b. as  
www.dummychat.com, RAVINDRANAUTH  
RAMKISSOON c.o.b. as www.infusioncanada.com,  
RAVINDRANAUTH RAMKISSOON c.o.b. as  
www.infusioncanada.ca, RAVINDRANAUGH  
RAMKISSOON c.o.b. as www.nfusiononline.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
www.nfusionrepair.com, RAVINDRANAUTH  
RAMKISSOON c.o.b. as  
www.nfusionwarrantycenter.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
www.nuvenio.ca, RAVINDRANAUGH  
RAMKISSOON c.o.b. as www.infusiondepo.com,  
RAVINDRANAUGH RAMKISSOON c.o.b. as  
DIGITAL R US, ANTHONY RAMKISSOON,  
ROSELINE RAMKISSOON, DIGITAL STORE  
INC., E-CANADA SOLUTIONS INC., JOHN DOE,  
JANE DOE and other persons unknown who have  
conspired with the name Defendants

Defendants  
CUMMING J.

Released: February 23, 2010

TOTAL P.022